前　言

在解决一个数学问题时，如果我们没有获得成功，原因常常在于我们没有认识到更一般的观点，从这种观点看来，眼下要解决的问题不过是一连串有关问题中的一个环节．采用这样的观点之后，不仅我们所研究的问题会容易得到解决，同时还会获得一种能应用于有关问题的普遍方法……

希尔伯特：《数学问题》，1900 年在巴黎第二届国际数学家大会上的演讲

本书中要讲的问题是："平方和"．

正整数是否都可写成两个整数的平方和？通过简单的试验便可知道，例如从 1 到 30 这三十个正整数中，3，6，7，11，12，14，15，19，21，22，23，24，27，28 和 30 这十五个数不能表成两个整数的平方和，而其余十五个整数是可以的（例如 $1=1^2+0^2$，$2=1^2+1^2$，$4=2^2+0^2$，$5=2^2+1^2$，等等）．那么，究竟什么样的正整数可以表成两个整数的平方和？

正整数是否都可写成三个整数的平方和？仍然作简单的试验便可知道，在不能表成两个整数平方和的上面那十五个数当中，除了 7，15，23 和 28 之外，其余十一个数均可表成三个整数的平方和（例如 $3=1^2+1^2+1^2$，$6=1^2+1^2+2^2$，$11=1^2+1^2+3^2$等等），而 7，15，23 和 28 均不是三个整数的平方和．

那么，究竟什么样的正整数可以表成三个整数的平方和？

7, 15, 23 和 28 不能表成三个整数的平方和，但是都可以表成四个整数的平方和：$7=1^2+1^2+1^2+2^2$, $15=1^2+1^2+2^2+3^2$, $23=1^2+2^2+3^2+3^2$, $28=1^2+1^2+1^2+5^2$. 换句话说，30 以内的正整数均可表成四个整数的平方和. 如果你愿意试验一下更大的正整数，便会发现它们似乎都可以. 那么，是否每个正整数均可表成四个整数的平方和呢？

更进一步，一个正整数 n 有多少种不同的方法可表成二个（三个或四个……）整数的平方和？例如 $25=(\pm5)^2+0^2=0^2+(\pm5)^2=(\pm3)^2+(\pm4)^2=(\pm4)^2+(\pm3)^2$ 共有 12 种方法表成二整数平方和. 将 n 表成二个（三个或四个……）整数平方和的表法数有没有简单的计算公式？

-1（以及所有负整数）显然不能表成整数的平方和，-1 也不能表成有理数或者实数的平方和. 但是在复数域中，-1 显然是平方和：$-1=0^2+i^2$，因 $i^2=-1$. 那么，给了任意一个域 F，如何判别 -1 是否为域 F 中元素的平方和？如果 -1 是域 F 中元素的平方和，那么 -1 至少是域 F 中几个元素的平方和？如果 -1 不是 F 中元素的平方和，那么域 F 中什么样的元素才是 F 中元素的平方和？

一个实系数多项式 $f(x_1, x_2, \cdots, x_n)$ 是否可表成一些实系数多项式的平方和？如果 $f(x_1, x_2, \cdots, x_n)$ 可如此表示，即 $f(x_1, x_2, \cdots, x_n)=g_1(x_1, x_2, \cdots, x_n)^2+g_2(x_1, x_2, \cdots, x_n)^2+\cdots+g_m(x_1, x_2, \cdots, x_n)^2$，其中 $g_1, g_2, \cdots, g_m$ 均是实系数多项式，那么对于任意实数 $a_1, a_2, \cdots, a_n$，$f(a_1, a_2, \cdots, a_n)=g_1(a_1, a_2, \cdots, a_n)^2+g_2(a_1, a_2, \cdots, a_n)^2+\cdots+g_m(a_1, a_2, \cdots, a_n)^2\geqslant0$. 对于任意实数都取非负值的多项式叫作正定的. 那么，反过来，正定的实系数多项式是否一定可表成一些实系

数多项式的平方和?如果不能,那么它是否可表成一些实系数有理函数的平方和?……

这些关于“平方和”的数学问题听起来通俗易懂,但其实都是很不简单的,每个问题的背后都有精彩的数学典故.首先,这些问题都是由著名数学家进行研究并得到解决的.关于正整数表成二整数平方和问题,早在公元前丢番图就作过研究.费尔马于1642年在给梅森(Mersenne)的信中就已基本上猜出了正确的结论,欧拉也研究过这个问题.但是第一个完全解决二整数平方和与三整数平方和问题的是德国大数学家高斯(1801年,24岁).而四整数平方和问题则是由法国数学家拉普拉斯解决的(1772年,23岁).他证明了:每个正整数均可表成四整数平方和.关于 -1 在域 F 中是否为平方和这个问题,德国数学家阿廷(E. Artin)和施莱尔(Schreier)于1926年进行了深刻的研究.而 -1 在域 F 中表成平方和所需最少元素个数,德国数学家费斯特(Pfister)于1967年给出十分漂亮的结果.关于正定实系数多项式是否可表成实系数多项式平方和,是由德国大数学家希尔伯特于1888年进行研究,答案在多数情形均是否定的.这促使他退一步问:正定实系数多项式是否一定可表成实系数有理函数的平方和?这是他于1900年巴黎第二届国际数学家大会上所提的二十三个著名数学问题中的第十七问题.这问题于1927年由阿廷所解决.本书将介绍这几段很不简单的数学史.

其次,上述数学家在研究和解决各种平方和问题的时候,提出和创造了新的数学思想和方法.这些新的数学思想和方法对于推动数学发展所起的作用和巨大意义,甚至超过了解决某些具体数学问题本身的价值.正如我们在前言一开头引用的希尔伯特那段话所指出的,这些数学家以高观点来考察

平方和问题，把它作为更一般问题的一个环节，创造了研究和解决更广泛问题的普遍方法，甚至由此产生出一些富有生命力的新的数学分支。高斯研究二整数平方和问题的方法，经过库默尔和希尔伯特等人的发展，形成了数论一个新的分支——代数数论。爱森斯坦等人对于整数平方和表法个数公式的研究，产生了椭圆模函数理论和模形式理论。阿廷和施莱尔对于-1是否为平方和的研究，建立了形式实域理论。正是利用这个理论，一年后阿廷解决了希尔伯特第十七问题。费斯特对-1表成平方和所需最少元素个数等问题的研究，建立了新的二次型代数理论……通过各种平方和问题，本书也想向大家介绍这些数学家创造了哪些新的数学思想和方法，如何推动数学的发展，并由此建立了哪些新的数学分支。

最后，我们所以能够为中学师生写这本小册子，是因为关于平方和的数学问题、数学结果，甚至相当一部分数学证明都是非常初等的。我们所选取的材料就所需知识面来讲均属于初等数学范围。除了中学教材之外，只需要一点初等数论知识。为了读者方便，本书将这些初等数论知识写成一个简单的附录，放在书后供大家参考。如果说大家有什么困难，可能会是数学修养方面的问题。而本书的主要目的正是想通过平方和问题使大家开阔眼界。我们试图通过对平方和这些初等数学材料讲述非初等的数学思想，把这些材料当作通向了解高等数学思想方法的媒介和桥梁，以提高中学师生的数学修养，了解近代数学的一些侧面和轮廓。除此之外，我们也希望大家从中领略到一点数学美。

冯克勤

一九八九年二月于合肥

目　录

一、整数平方和——能表示吗？

设 k 是一个正整数．本节要解决的问题是：哪些正整数 n 可以表示成 k 个整数的平方和？以后把"k个整数的平方和"简称为"k 平方和"．

一平方（和）问题是很平凡的．若 n 为某个整数的平方，则 n 叫作完全平方数．设

$$n=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$$

是 n 的标准素因子分解式（见附录），则 n 为完全平方数，当且仅当 $r_1, r_2, \cdots, r_s$ 均为偶数．而一般地，每个正整数 n 均可唯一地表示成

$$n=m^2m',$$

其中 m 为正整数，而 m' 不被任何素数的平方除尽．也就是说，m' 或者为 1，或者是一些彼此不同的素数的乘积．我们将 m^2 和 m' 分别叫作 n 的平方因子部分和无平方因子部分．

以下从二平方和问题谈起．

1. 二平方和——高斯定理

正整数 n 是否为二平方和，相当于说不定方程

$$x^2+y^2=n$$

是否有整数解 (x, y)．这个问题丢番图（公元前 409－325）就

研究过. 例如他发现了下面的恒等式:

$$(a^2+b^2)(c^2+d^2)=(ac\mp bd)^2+(bc\pm ad)^2. \quad ①$$

大家可以将两边展开直接验证这个恒等式的正确性, 也可以像高斯一样利用复数:

$$\text{左边}=|a+bi|^2\cdot|c\pm di|^2=|(a+bi)(c\pm di)|^2$$

$$=|(ac\mp bd)+(bc\pm ad)i|^2=\text{右边}.$$

并且由这个恒等式直接得到如下重要结论:

引理1 若正整数 n 和 m 均是二平方和, 则 nm 也是二平方和. 于是(用数学归纳法即可证出)任意有限个二平方和之积仍是二平方和.

从这个引理自然会使我们想到首先需弄清哪些素数是二平方和. 因为若所有的素数均是二平方和, 那么由引理1和正整数的素因子分解特性, 便可推出每个正整数均为二平方和了. 但不幸(也许是更为有趣)的是: 不是所有的素数均为二平方和. 下面的定理圆满地解决了"素数何时为二平方和"这个问题. 虽然费尔马 (Fermat, 1601—1665) 等人早就提出这个结论, 但是第一个证明被高斯认为是由欧拉(Euler, 1707—1783)给出的.

定理1 (欧拉) 素数 p 是二平方和的充分必要条件为 $p=2$ 或者 $p\equiv1(\mathrm{mod}\,4)$. (换句话说: 素数 p 不为二平方和 $\Leftrightarrow$ $p\equiv3(\mathrm{mod}\,4)$.)

证明 必要性的证明是容易的. 由于 $2=1^2+1^2$, 以下设 p 是奇素数. 如果 p 是二平方和, 即 $p=x^2+y^2$, 其中 x 和 y 是整数. 则 $x^2+y^2\equiv0(\mathrm{mod}\,p)$, 即 $x^2\equiv-y^2(\mathrm{mod}\,p)$. 易知 $p\nmid y$, 于是同余式两边可同时除以 y^2, 得到 $\left(\frac{x}{y}\right)^2\equiv-1(\mathrm{mod}\,p)$. 这意味着 -1 是模 p 的二次剩余. 因此 $p\equiv1(\mathrm{mod}\,4)$ (见附录),

这就证明了必要性.

充分性的证明就困难多了. 我们要证明当 $p\equiv1(\bmod 4)$ 时, p 是二平方和. 首先, 由 $p\equiv1(\bmod 4)$ 知 -1 为模 p 的二次剩余, 即有整数 a 使得

$$a^2\equiv-1(\bmod p).$$

a 所属模 p 同余类中每个整数均有这个性质, 而这个同余类中总有一个整数的绝对值小于 $\frac{p}{2}$(见附录), 从而我们不妨假定 $|a|<\frac{p}{2}$. 于是 $p|a^2+1$, 即 $a^2+1=mp$, 其中 m 为正整数, 并且 $mp=a^2+1<\left(\frac{p}{2}\right)^2+1<p^2$, 从而 $1\leqslant m\leqslant p-1$. 至此, 我们证明了一个初步结果: 在 $1, 2, \cdots, p-1$ 当中存在整数 m, 使得 mp 为二平方和.

现在我们以 m_0 表示使得 m_0p 为二平方和的最小正整数. 由上面所证可知 m_0 是存在的, 并且 $1\leqslant m_0\leqslant p-1$. 我们的目的显然是要证 $m_0=1$(从而 p 为二平方和). 证明用反证法: 如果 $m_0\geqslant2$, 而 $m_0p=x_1^2+y_1^2$, 其中 x_1 和 y_1 为整数, 在 x_1 和 y_1 所属的模 m_0 同余类中总可分别取整数 x_0 和 y_0, 使得 $|x_0|$ 和 $|y_0|$ 均不超过 $\frac{m_0}{2}$, (为什么可以这样做?) 即

$$x_0\equiv x_1,\ y_0\equiv y_1(\bmod m_0)\quad \left(|x_0|,\ |y_0|\leqslant\frac{m_0}{2}\right).$$

如果 $x_0=y_0=0$, 则导致 $m_0|p$. 但这与 $1\leqslant m_0\leqslant p-1$ 矛盾, 因此 x_0 和 y_0 不全为零, 即

$$0<x_0^2+y_0^2\leqslant\left(\frac{m_0}{2}\right)^2+\left(\frac{m_0}{2}\right)^2=\frac{m_0^2}{2}.$$

由于 $\qquad x_0^2+y_0^2\equiv x_1^2+y_1^2=m_0p\equiv0(\bmod m_0),$

可知 $x_0^2+y_0^2=m'm_0$, 其中 m' 为整数. 并且由 $0<x_0^2+y_0^2=$

$m'm_0 \leqslant \frac{m_0^2}{2}$ 可知 $1 \leqslant m' \leqslant \frac{m_0}{2} < m_0$. 再由恒等式 ① 得出

$$m'm_0^2p = (x_0^2+y_0^2)(x_1^2+y_1^2)$$
$$= (x_0x_1+y_0y_1)^2+(x_0y_1-y_0x_1)^2.$$

但是 $$x_0x_1+y_0y_1 \equiv x_1^2+y_1^2 \equiv 0 \pmod{m_0},$$
$$x_0y_1-y_0x_1 \equiv x_1y_1-y_1x_1 = 0 \pmod{m_0}.$$

因此 $A=\frac{1}{m_0}(x_0x_1+y_0y_1)$ 和 $B=\frac{1}{m_0}(x_0y_1-y_0x_1)$ 均是整数，并且 $A^2+B^2=\frac{m'm_0^2p}{m_0^2}=m'p$，即 $m'p$ 也是二平方和. 但是 $1 \leqslant m' < m_0$，这便与 m_0 的最小性相矛盾. 唯一的可能性便是 $m_0=1$，即 p 为二平方和. 这就完成了定理 1 的证明.

上述证明的后一部分采用的方法是费尔马首创的，叫作"无穷递降法". 因为它的证明实质是：如果 m_0p 为二平方和并且 $m_0 \geqslant 2$，则求出另一正整数 $m_1(=m') < m_0$，使得 m_1p 也为二平方和. 如果仍旧 $m_1 \geqslant 2$，则按同样办法又可找到正整数 $m_2 < m_1$，使得 m_2p 也为二平方和，……于是我们得到递降的正整数序列 $m_0 > m_1 > m_2 > \cdots$. 但它们均是正整数，从而不能无穷递降下去，所以必然经过有限步达到值 1. 我们以后在研究四平方和问题时还要用到这个方法.

现在讨论任意正整数 n 何时为二平方和. 下面定理给出完整的答案，结论本身也是于十七世纪由费尔马等人猜测出来，但是第一个证明是由高斯 (Gauss, 1777—1855) 于 1801 年给出的.

定理 2（高斯） 正整数 n 是二平方和的充分必要条件为：n 的无平方因子部分 m' 或者为 1，或者 m' 的每个素因子均是二平方和（由定理 1，这意味着 m' 的每个素因子均为 2

或模 4 余 1 的素数)

证明 充分性是容易的：设 $n=m^2m'$，如果 m' 的每个素因子均是二平方和，由引理 1 知 m' 为二平方和，而 $m^2=m^2+0^2$ 为二平方和，从而 $n=m^2m'$ 为二平方和.

现在证明必要性，即若 n 为二平方和，则 n 的无平方因子部分 m' 或者为 1，或者 m' 的每个素因子均是二平方和. 我们对 n 作数学归纳法. 当 $n=1$ 时命题显然成立. 现设命题对所有小于 n 的正整数均正确，而 n 为二平方和：$n=x^2+y^2$，我们要证 m' 的所有素因子均为二平方和. 如果 n 的所有素因子均为二平方和，则 m' 的素因子也是如此，从而证毕. 下设 n 有素因子 p 不是二平方和. 由定理 1 知 $p\equiv 3 \pmod 4$，于是 $x^2+y^2=n\equiv 0 \pmod p$. 如果 $p\nmid x$，则 $\left(\frac{y}{x}\right)^2\equiv -1 \pmod p$，这在 $p\equiv 3 \pmod 4$ 时是不可能的，因此 $p\mid x$. 同样地 $p\mid y$. 于是 $p^2\mid x^2+y^2=n$，即 $n'=\frac{n}{p^2}$ 是整数，并且由 $n'=\left(\frac{x}{p}\right)^2+\left(\frac{y}{p}\right)^2$ 知 n' 为二平方和. 由归纳假设知 n' 的无平方因子部分的每个素因子均是二平方和. 但是易知 $n'=\frac{n}{p^2}$ 和 n 具有同样的无平方因子部分 m'，这就证明了定理 2.

【例】 1989 和 1990 是否为二平方和？

解：$1989=3^2\cdot 13\cdot 17$，无平方因子部分为 $m'=13\cdot 17$. 由于 $13\equiv 17\equiv 1 \pmod 4$，从而 1989 是二平方和. 事实上，由于 $13=2^2+3^2$, $17=1^2+4^2$，于是

$$
\begin{aligned}
1989&=3^2\cdot|2+3i|^2\cdot|1+4i|^2\\
&=3^2\cdot|(2+3i)(1+4i)|^2=3^2\cdot|-10+11i|^2\\
&=3^2(10^2+11^2)=30^2+33^2,
\end{aligned}
$$

或者 $1989=3^2\cdot|(2-3i)(1+4i)|^2=3^2\cdot|14+5i|^2$

$$=42^2+15^2.$$

而 $1990=2\cdot5\cdot199$，其中 199 为素数并且 $199\equiv3\pmod 4$，由定理 2 知 1990 不是二平方和.

从上面例子可以看出，一个正整数 n 可能有许多种表成二平方和的方法．即不定方程 $n=x^2+y^2$ 可能有许多整数解 (x,y)．如 1989 就有 16 种方式表示成二平方和 x^2+y^2，其中

$$(x,y)=(\pm30,\ \pm33),\ (\pm33,\ \pm30),$$
$$(\pm42,\ \pm15),\ (\pm15,\ \pm42).$$

而本质上则只有两种解：$(x,y)=(30,33)$ 和 $(42,15)$，其他解均可由这两个解加上负号或交换 x 和 y 的取值而得到．一般地，正整数 n 共有多少方法表示成二平方和，则是比"能否表成二平方和"更为深入的问题，我们将它留在下章讨论．但目前可以对 n 为素数的情形解决此问题．由于 $2=1^2+1^2$ 本质上只有一种表示方法．以下只需再讨论 p 是模 4 余 1 的素数．

定理 3(高斯) 设 p 是素数，并且 $p\equiv1\pmod 4$，则 p 本质上只有一种方法表成二平方和.

证明 设 $p=a^2+b^2=A^2+B^2$，其中 $a,\ b,\ A,\ B$ 均为正整数．我们只需证明 $a=A$ 或者 $a=B$ 即可．由于

$$p^2=(a^2+b^2)(A^2+B^2)=(aA\pm bB)^2+(aB\mp bA)^2, \quad ②$$

$$(aA+bB)(aA-bB)=A^2(a^2+b^2)-b^2(A^2+B^2)$$
$$=A^2p-b^2p\equiv0 \pmod p,$$

从而 $p|aA+bB$ 或者 $p|aA-bB$．如果 $p|aA+bB$，注意 $aA+bB>0$，由②式可知必然 $aA+bB=p$，$aB-bA=0$．于是

$$\frac{a^2}{A^2}=\frac{b^2}{B^2}=\frac{a^2+b^2}{A^2+B^2}=\frac{p}{p}=1.$$

因此 $a=A$, $b=B$. 同样若 $p\mid aA-bB$, 则由 $aB+bA>0$ 及②式可知 $aB+bA=p$, $aA-bB=0$. 仿上面证明即得 $a=B$, $b=A$. 证毕.

练习 求证: 若正整数 n 可表成两个有理数的平方和, 则必可表成两个整数的平方和(提示: 用定理 2).

2. 四平方和——兼谈域和四元数体

我们在上节圆满解决了二平方和问题. 接下来应当是三平方和问题. 但是四平方和问题有非常漂亮的结果, 并且证明与定理 2 的证明非常相像, 所以先讲它. 1770 年, 拉格朗日(Lagrange, 1736—1813)第一个证明了下面的定理.

定理 4(拉格朗日) 每个正整数均是四平方和.

证明 首先请大家验证下面的恒等式:

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)$$
$$=A^2+B^2+C^2+D^2, \qquad ③$$

其中
$$\begin{cases}A=x_1y_1+x_2y_2+x_3y_3+x_4y_4,\\ B=x_1y_2-x_2y_1-x_3y_4+x_4y_3,\\ C=x_1y_3+x_2y_4-x_3y_1-x_4y_2,\\ D=x_1y_4-x_2y_3+x_3y_2-x_4y_1.\end{cases} \qquad ④$$

由恒等式③可知, 有限多个四平方和的乘积仍旧为四平方和. 因此我们只需证每个素数 p 均为四平方和即可. 由于 $2=1^2+1^2+0^2+0^2$, 以下设 p 为奇素数. 考虑集合

$$M=\left\{x^2 \mid x=0,\ 1,\ 2,\ \cdots,\ \frac{p-1}{2}\right\},$$

$$N=\left\{-(1+y^2) \mid y=0,\ 1,\ 2,\ \cdots,\ \frac{p-1}{2}\right\}.$$

集合 M 中 $\frac{p+1}{2}$ 个数模 p 彼此不同余. 因若 $x_1^2\equiv x_2^2 \pmod{p}$, $0\leqslant x_1<x_2\leqslant\frac{p-1}{2}$, 则 $p \mid (x_1+x_2)(x_2-x_1)$. 但是

$$1\leqslant x_2\pm x_1\leqslant\frac{p-1}{2}+\frac{p-1}{2}=p-1,$$

这就导出矛盾. 同样地, 集合 N 中 $\frac{p+1}{2}$ 个数模 p 也彼此不同余. 但是 M 和 N 元素个数合在一起为 $\frac{p+1}{2}+\frac{p+1}{2}=p+1$, 而模 p 同余类只有 p 个. 从而集合 M 中必有某个 x^2 和集合 N 中某个 $-(1+y^2)$ 是模 p 同余的. 即存在整数 x 和 y 使得 $0\leqslant x,\ y\leqslant\frac{p-1}{2}$, 并且 $x^2\equiv-(1+y^2) \pmod{p}$, 即 $x^2+y^2+1\equiv 0 \pmod{p}$. 于是有正整数 m, 使得

$$mp=x^2+y^2+1=x^2+y^2+1^2+0^2.$$

并且由
$$x^2+y^2+1<\left(\frac{p}{2}\right)^2+\left(\frac{p}{2}\right)^2+1<p^2,$$

可知 $1\leqslant m\leqslant p-1$. 换句话说, 我们证明了: 存在整数 m, $1\leqslant m\leqslant p-1$, 使得 mp 为四平方和.

接下来又和定理 2 的证明一样, 用无穷递降法. 以 m_0 表示使得 m_0p 为四平方和的最小正整数. 由上面所证知这样的 m_0 是存在的, 并且 $1\leqslant m_0\leqslant p-1$. 我们的目的是证明 $m_0=1$. 若不然, 即若 $m_0\geqslant 2$, 设 $m_0p=x_1^2+x_2^2+x_3^2+x_4^2$, 其中 $x_1,\ x_2,\ x_3,\ x_4$ 均为整数. 如果 m_0 是偶数, 则

$$\begin{aligned}x_1+x_2+x_3+x_4&\equiv x_1^2+x_2^2+x_3^2+x_4^2\\&=m_0p\equiv 0 \pmod{2}.\end{aligned}$$

在 x_1, x_2, x_3, x_4 中至少有两个数同时为偶或同时为奇. 不妨设它们为 x_1 和 x_2, 则 $x_1\equiv x_2 \pmod 2$. 再由上面同余式即知 $x_3\equiv x_4 \pmod 2$. 于是 $\frac{1}{2}(x_1\pm x_2)$ 和 $\frac{1}{2}(x_3\pm x_4)$ 均是整数, 并且

$$\frac{m_0}{2}p=\left(\frac{x_1+x_2}{2}\right)^2+\left(\frac{x_1-x_2}{2}\right)^2 +\left(\frac{x_3+x_4}{2}\right)^2+\left(\frac{x_3-x_4}{2}\right)^2,$$

即 $\frac{m_0}{2}p$ 为四平方和. 这与 m_0 的最小性相矛盾. 所以 m_0 必为奇数. 这时, 存在整数 y_i, 使得

$$y_i\equiv x_i \pmod{m_0},\ |y_i|<\frac{m_0}{2}\quad (i=1, 2, 3, 4).$$

如果 $y_i(1\leqslant i\leqslant 4)$ 均为 0, 则 $m_0|x_i(1\leqslant i\leqslant 4)$. 从而 $m_0^2|x_1^2+x_2^2+x_3^2+x_4^2=m_0p$, 于是 $m_0|p$, 这与 $2\leqslant m_0\leqslant p-1$ 相矛盾. 因此 $y_i(1\leqslant i\leqslant 4)$ 不全为零, 即

$$1\leqslant y_1^2+y_2^2+y_3^2+y_4^2<4\cdot\left(\frac{m_0}{2}\right)^2=m_0^2.$$

又由于 $$y_1^2+y_2^2+y_3^2+y_4^2\equiv x_1^2+x_2^2+x_3^2+x_4^2 =m_0p\equiv 0 \pmod{m_0},$$

于是 $y_1^2+y_2^2+y_3^2+y_4^2=m'm_0$, 其中 m' 为整数, 并且

$$1\leqslant m'm_0<m_0^2,\quad 即\quad 1\leqslant m'<m_0.$$

现在利用恒等式③:

$$m'm_0^2p=(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) =(A^2+B^2+C^2+D^2),$$

其中 A, B, C, D 的表达式如④式所示. 我们有

$$A=x_1y_1+x_2y_2+x_3y_3+x_4y_4 \equiv x_1^2+x_2^2+x_3^2+x_4^2=m_0p\equiv 0 \pmod{m_0},$$

$$B=x_1y_2-x_2y_1-x_3y_4+x_4y_3$$
$$\equiv x_1x_2-x_2x_1-x_3x_4+x_4x_3\equiv 0 \pmod{m_0},$$

同样地有 $C\equiv D\equiv 0 \pmod{m_0}$. 从而

$$m'p=\left(\frac{A}{m_0}\right)^2+\left(\frac{B}{m_0}\right)^2+\left(\frac{C}{m_0}\right)^2+\left(\frac{D}{m_0}\right)^2$$

是将 $m'p$ 表成四个整数平方和. 但是 $1\leqslant m'<m_0$, 这与 m_0 的最小性相矛盾. 因此必然 $m_0=1$, 即 p 为四平方和. 这就完成了定理 4 的证明.

拉格朗日定理是这样漂亮, 以至于我们对它本身已没有话要说, 只好再说些题外的话. 首先, 由于 7 不是三平方和, 从而使每个正整数均为 k 平方和的最小 k 值是 4. 其次, 进一步要问: 每个正整数 n 表成四平方和共有多少种方法? 这也留到下节研究. 最后, 让我们回过头来看一下恒等式 ③. 这个恒等式的直接验证并不难, 初中学生都应当会作. 问题是这个恒等式是怎样发现的? 因为科学的本质在于发现新事物, 而验证是第二位的. 这个问题有历史上的兴趣, 我们也想结合这个数学典故给大家谈谈"域"这个概念.

高斯利用复数 $i^2=-1$ 证明了关于二平方和的恒等式 ①. 高斯的观点是: 将求不定方程 $n=x^2+y^2$ 的整数解这个纯属整数范围内的问题, 放到复数集合上来考察, 即写成 $n=|x+iy|^2$. 而恒等式 ① 的证明不过利用了关于复数绝对值的一个简单事实: 任意二复数的绝对值之积等于它们之积的绝对值, 即 $|\alpha|\cdot|\beta|=|\alpha\beta|$. 我们是否能找到一个别的什么"数"的集合代替复数集合, 然后用这种新的数集合的性质证明恒等式 ③?

复数集合中是可以进行加减乘除四则运算的 (其中作除法时除数不为 0). 并且加法和乘法满足结合律、交换律和分

配律. 这样的代数结构在近世代数中叫作域. 今后把复数域记作 $\mathbf{C}$. 事实上, $\mathbf{C}$ 有许多子集合也是域, 如有理数域 $\mathbf{Q}$、实数域 $\mathbf{R}$ 等等. 再比如, 设整数 d 不是完全平方数, 则 $\sqrt{d}$ 不是有理数. 令

$$\mathbf{Q}(\sqrt{d})=\{\alpha+\beta\sqrt{d}\mid\alpha,\ \beta\in\mathbf{Q}\},$$

这是比有理数域 $\mathbf{Q}$ 更大的域. 请大家验证集合 $\mathbf{Q}(\sqrt{d})$ 满足域的上述所有条件. 这里我们只举例验证 $\mathbf{Q}(\sqrt{d})$ 中可作除法: 设 $\alpha+\beta\sqrt{d}$ 和 $\gamma+\delta\sqrt{d}$ 均属于 $\mathbf{Q}(\sqrt{d})$, 其中 $\alpha,\beta,\gamma,\delta\in\mathbf{Q}$, 并且 $\gamma+\delta\sqrt{d}\neq0$. 因此 γ 和 δ 不全为 0. 由 d 不是完全平方数可知

$$(\gamma+\delta\sqrt{d})(\gamma-\delta\sqrt{d})=\gamma^2-\delta^2d\neq0,$$

因此
$$\frac{\alpha+\beta\sqrt{d}}{\gamma+\delta\sqrt{d}}=\frac{(\alpha+\beta\sqrt{d})(\gamma-\delta\sqrt{d})}{\gamma^2-d\delta^2}=\frac{\alpha\gamma-\beta\delta d}{\gamma^2-d\delta^2}+\frac{\beta\gamma-\alpha\delta}{\gamma^2-d\delta^2}\sqrt{d}.$$

而 $\dfrac{\alpha\gamma-\beta\delta d}{\gamma^2-d\delta^2}$ 和 $\dfrac{\beta\gamma-\alpha\delta}{\gamma^2-d\delta^2}$ 均是有理数, 即 $\dfrac{\alpha+\beta\sqrt{d}}{\gamma+\delta\sqrt{d}}$ 属于 $\mathbf{Q}(\sqrt{d})$. 从而 $\mathbf{Q}(\sqrt{d})$ 中可作除法.

我们前面所谈的域都是比复数域 $\mathbf{C}$ 小的域. 那么是否有比 $\mathbf{C}$ 更大的域呢? 设 x 是一个未定元(事实上, 只要 x 不是任何复系数多项式的根即可). 设 $f(x)$ 和 $g(x)$ 是两个复系数的(关于 x 的)多项式, 并且 $g(x)$ 不恒等于 0, 则 $\dfrac{f(x)}{g(x)}$ 叫作有理函数. 所有这种有理函数对于大家所学过的通常加减乘除运算形成一个域, 这叫作复数域 $\mathbf{C}$ 上的有理函数域, 表示成 $\mathbf{C}(x)$. 由于每个非零复数看成是零次多项式, 从而 $\mathbf{C}(x)$ 包含 $\mathbf{C}$, 即 $\mathbf{C}(x)$ 是比 $\mathbf{C}$ 更大的域. 类似地我们有实数域 $\mathbf{R}$ 上的有理函数域 $\mathbf{R}(x)$(即多项式系数均是实数), 有理数域 $\mathbf{Q}$ 上

的有理函数域 $\mathbf{Q}(x)$ 等等.

另一方面，是否有一种代数结构，它满足域的几乎所有性质，只是乘法不必满足交换律，即 ab 和 ba 不一定相等？这样的代数结构叫作体. 第一个这样的例子是由哈密尔顿(Hamilton, 1805—1865)发现的，叫作四元数体，表示成 $\mathbf{H}$. 它的每个元素(叫作四元数)写成形式

$$\alpha=x_1+x_2i+x_3j+x_4k,$$

其中 x_1, x_2, x_3, x_4 均是实数.

四元数的加减法采取通常形式，即

$$(x_1+x_1i+x_2j+x_3k)\pm(y_1+y_2i+y_3j+y_4k)$$
$$=(x_1\pm y_1)+(x_2\pm y_2)i+(x_3\pm y_3)j+(x_4\pm y_4)k.$$

而乘法则有以下的乘法表:

$$ij=k=-ji,\ jk=i=-kj,\ ki=j=-ik,$$
$$i^2=j^2=k^2=-1;$$

并且对每个实数 a 和每个四元数 α, $a\alpha=\alpha a$. 然后用分配律就可作任意两个四元数的乘积. 例如设 x_1, x_2, x_3, x_4 均为实数，则

$$\begin{aligned}(x_1+x_2i+x_3j+x_4k)&(x_1-x_2i-x_3j-x_4k)\\ &=x_1^2-x_2^2i^2-x_3^2j^2-x_4^2k^2+(x_2x_1-x_1x_2)i\\ &\quad+(x_3x_1-x_1x_3)j+(x_4x_1-x_1x_4)k\\ &\quad-x_2x_3(ij+ji)-x_3x_4(jk+kj)-x_4x_2(ki+ik)\\ &=x_1^2+x_2^2+x_3^2+x_4^2. \qquad ⑤\end{aligned}$$

我们把 $x_1-x_2i-x_3j-x_4k$ 叫作四元数 $\alpha=x_1+x_2i+x_3j+x_4k$ 的共轭，表示成 $\bar{\alpha}$. 而把实数 $(x_1^2+x_2^2+x_3^2+x_4^2)^{\frac{1}{2}}$ 叫作 α 的绝对值，表示成 $|\alpha|$. 那么公式⑤表明

$$\alpha\bar{\alpha}=\bar{\alpha}\alpha=|\alpha|^2.$$

如果 $\alpha\neq0$（即 x_1, x_2, x_3, x_4 不全为 0），则 $|\alpha|>0$．从而

$$\alpha\cdot\frac{\bar{\alpha}}{|\alpha|^2}=\frac{\bar{\alpha}}{|\alpha|^2}\cdot\alpha=1.$$

这表明 $\frac{\bar{\alpha}}{|\alpha|^2}=\frac{1}{x_1^2+x_2^2+x_3^2+x_4^2}(x_1-x_2i-x_3j-x_4k)$ 为 α 的乘法逆元素．于是对任意两个四元数 α 和 $\beta(\beta\neq0)$，则四元数 $\frac{1}{|\beta|^2}\alpha\bar{\beta}$ 和 $\frac{1}{|\beta|^2}\bar{\beta}\alpha$ 分别是方程 $\alpha=x\beta$ 和 $\alpha=\beta x$ 的解．这就表明四元数集合中有除法运算，不过由于乘法没有交换律（例如 $ij=-ji$！），方程 $\alpha=x\beta$ 和 $\alpha=\beta x$ 的解可能不同，所以我们不能将解写成 $\frac{\alpha}{\beta}$ 这种分式的形式．于是 $\mathbf{H}$ 是体．

设 $\alpha=x_1-x_2i-x_3j-x_4k$，$\beta=y_1+y_2i+y_3j+y_4k$，则可直接用分配律算出：

$$\alpha\beta=A+Bi+Cj+Dk, \qquad ⑥$$

其中 A, B, C, D 如 ④ 式所示．若将 x_i 改成 y_i，而将 y_i 改成 x_i，则 α 和 β 分别变成 $\bar{\beta}$ 和 $\bar{\alpha}$，而由 ④ 式知 A, B, C, D 分别变成 $A, -B, -C, -D$．于是 ⑥ 式变成

$$\bar{\beta}\cdot\bar{\alpha}=A-Bi-Cj-Dk=(\overline{\alpha\beta}).$$

从而
$$|\alpha\beta|^2=(\alpha\beta)(\overline{\alpha\beta})=(\alpha\beta)(\bar{\beta}\cdot\bar{\alpha})=\alpha(\beta\bar{\beta})\bar{\alpha}$$
$$=\alpha|\beta|^2\bar{\alpha}=\alpha\bar{\alpha}|\beta|^2=|\alpha|^2\cdot|\beta|^2.$$

但是
$$|\alpha\beta|^2=|A+Bi+Cj+Dk|^2$$
$$=A^2+B^2+C^2+D^2,$$
$$|\alpha|^2=x_1^2+x_2^2+x_3^2+x_4^2,\ |\beta|^2=y_1^2+y_2^2+y_3^2+y_4^2.$$

因此
$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)$$
$$=A^2+B^2+C^2+D^2.$$

正像用复数绝对值性质 $|\alpha\beta|=|\alpha|\cdot|\beta|$ 推出关于二平方和的

恒等式 ① 一样，我们用四元数体上绝对值的类似性质得到了关于四平方和的恒等式 ③.

3. 二元二次型

哪些正整数为三平方和，也有很简单的结论．但是证明需要更多的数论知识．目前已有许多种初等证明方法．我们在下一小节将要向大家介绍一种利用二次型的证法，这是因为三平方和表法个数的公式也与二元二次型有关．所以我们在本节中暂时离开三平方和问题，讲一点关于二元二次型的知识．

设 a, b, c 是不全为零的整数，形如

$$f(x, y)=ax^2+bxy+cy^2$$

的函数叫作二元二次型，简记为 $f=[a, b, c]$．而 $d=b^2-4ac$ 叫作 f 的判别式．二元二次型 $f(x, y)$ 叫作正定的，是指对任意不全为零的整数 A, B，均有 $f(A, B)>0$．下面给出二元二次型正定的判别法．

引理 2 二元二次型 $f(x, y)=[a, b, c]$ 正定的充分必要条件是 $a>0$ 并且 $d<0$.

证明 若 f 正定，则由定义即知 $a=f(1, 0)>0$．进而易知

$$f(x, y)=a\left[\left(x+\frac{b}{2a}y\right)^2+(-d)\left(\frac{y}{2a}\right)^2\right], \qquad ⑦$$

于是 $f(-b, 2a)=-ad>0$，即 $d<0$．反之若 $a>0$ 并且 $d<0$，则由 ⑦ 可知对任意整数 x, y 均有 $f(x, y)\geqslant 0$．并且 $f(x, y)=0\leftrightarrow x+\frac{b}{2a}y=0$ 同时 $\frac{y}{a}=0\leftrightarrow y=0$ 同时 $x=0$．这就表明

当 x 和 y 不全为 0 时，$f(x, y)>0$. 即 f 是正定的. 证毕.

设 $f(x, y)=ax^2+bxy+cy^2$，作变量代换

$$\begin{cases} x=Px'+Qy', \\ y=Rx'+Ty', \end{cases}$$

便得到一个新的(关于 x', y' 的)二元二次型

$$\begin{aligned} g(x', y') &= f(Px'+Qy', Rx'+Ty') \\ &= a(Px'+Qy')^2+b(Px'+Qy')(Rx'+Ty') \\ &\quad +c(Rx'+Ty')^2 \\ &= a'x'^2+b'x'y'+c'y'^2=[a', b', c'], \end{aligned}$$

其中

$$\begin{cases} a'=g(1, 0)=f(P, R)=aP^2+bPR+cR^2, \\ c'=g(0, 1)=f(Q, T)=aQ^2+bQT+cT^2, \\ b'=g(1, 1)-a'-c'=2aPQ+b(PT+QR)+2cRT. \end{cases} \tag{8}$$

请大家验证(又是恒等式!)$g(x', y')$ 的判别式为

$$\begin{aligned} d'=b'^2-4a'c' &= (b^2-4ac)(PT-QR)^2 \\ &= d(PT-QR)^2. \end{aligned} \tag{9}$$

特别当 $PT-QR=\begin{vmatrix} P & Q \\ R & T \end{vmatrix}=1$ 时，$d'=d$. 即这时二元二次型 f 和 g 有相同的判别式.

定义 设 $f(x, y)$ 和 $g(x, y)$ 是两个二元二次型. 如果存在整数 P, Q, R, T，使得 $PT-QR=1$，并且

$$g(x, y)=f(Px+Qy, Rx+Ty),$$

我们称 f 与 g 等价，表示成 $f\sim g$.

【例 1】 设 $f(x, y)=ax^2+bxy+cy^2=[a, b, c]$. 取 $(P, Q, R, T)=(0, 1, -1, 0)$，则 $PT-QR=1$. 于是 $[a, b, c]$ 与

$$\begin{aligned} g(x, y)=f(y, -x) &= ay^2-bxy+cx^2 \\ &= [c, -b, a] \end{aligned}$$

等价.

【例2】 设$f=[a, b, c]$. 取$(P, Q, R, T)=(1, m, 0, 1)$, 其中$m$为任意整数. 则$PT-QR=1\cdot 1-m\cdot 0=1$. 于是$[a, b, c]$与

$$\begin{aligned}g(x, y)=f(x+my, y)&=a(x+my)^2\\&\quad+b(x+my)y+cy^2\\&=[a, 2am+b, am^2+bm+c]\end{aligned}$$

等价.

引理3 (等价性质)设f, g, h均为二元二次型. 则

(i)(自反性) 每个二元二次型均与自身等价. 即$f\sim f$.

(ii) (对称性) 若f与g等价,则g与f等价. 即:若$f\sim g$,则$g\sim f$.

(iii)(传递性) 若f与g等价, 而g又与h等价, 则f与h等价. 即:若$f\sim g$, $g\sim h$,则$f\sim h$.

证明 (i)变量代换中取$(P, Q, R, T)=(1, 0, 0, 1)$即知$f\sim f$.

(ii) 若$f\sim g$, 则有整数P, Q, R, T, $PT-QR=1$, 使得$g(x, y)=f(x', y')$,其中

$$\begin{cases}x'=Px+Qy,\\ y'=Rx+Ty.\end{cases}$$

由于这个二元一次方程组的行列式$\begin{vmatrix}P & Q\\ R & T\end{vmatrix}=1\neq 0$,从而可解出$x$和$y$来:

$$x=\frac{\begin{vmatrix}x' & Q\\ y' & T\end{vmatrix}}{\begin{vmatrix}P & Q\\ R & T\end{vmatrix}}=Tx'-Qy',\quad y=\frac{\begin{vmatrix}P & x'\\ R & y'\end{vmatrix}}{\begin{vmatrix}P & Q\\ R & T\end{vmatrix}}=-Rx'+Py'.$$

于是 $f(x', y') = g(Tx' - Qy', -Rx' + Py')$. 并且

$$\begin{vmatrix} T & -Q \\ -R & P \end{vmatrix} = PT - QR = 1,$$

这就表明 $g \sim f$.

(iii) 若 $f \sim g$, $g \sim h$, 则

$$g(x, y) = f(Ax + By, Cx + Dy),$$
$$h(x', y') = g(A'x' + B'y', C'x' + D'y'),$$

其中 $AD - BC = A'D' - B'C' = 1$. 于是

$$\begin{aligned} h(x', y') &= f(A(A'x' + B'y') + B(C'x' + D'y'), \\ &\qquad C(A'x' + B'y') + D(C'x' + D'y')) \\ &= f((AA' + BC')x' + (AB' + BD')y', \\ &\qquad (CA' + DC')x' + (CB' + DD')y'), \end{aligned}$$

由于 $\begin{vmatrix} AA' + BC' & AB' + BD' \\ CA' + DC' & CB' + DD' \end{vmatrix} = \begin{vmatrix} A & B \\ C & D \end{vmatrix} \cdot \begin{vmatrix} A' & B' \\ C' & D' \end{vmatrix}$

$= 1 \cdot 1 = 1,$

这就表明 $f \sim h$. 证毕.

从引理 3 可知, 二元二次型全体可以分成许多互不相交的子集合, 每个子集合中的二元二次型彼此等价, 而不同子集合中的二元二次型是不等价的. 每个子集合叫作二元二次型的一个等价类.

同一等价类中的二元二次型有什么公共性质呢? 首先, 由前所述(见公式 ⑨), 等价的二元二次型有相同的判别式. 即判别式是等价类的"不变量". 于是, 判别式不同的两个二元二次型是不能等价的. 进而, 设 $f(x, y) = [a, b, c]$是正定的, 由引理 2 可知 $a > 0$, $d = b^2 - 4ac < 0$. 设 $g(x, y) = [a', b', c']$与 f 等价, 则有整数 P, Q, R, T, $PT - QR = 1$, 使得 $g(x, y) = f(Px + Qy, Rx + Ty)$. 由 ⑧ 式知 $a' = f(P, R) > 0$

(因为 f 是正定的，并且由 $PT-QR=1$ 知 P 和 R 不全为零)，而 g 的判别式 $=f$ 的判别式 $=d<0$. 再由引理 2 即知 g 也是正定的. 换句话说，正定二元二次型只能与正定二元二次型等价. 即二元二次型是否正定也是等价类的性质. 等价类另一个重要的性质是可表示的数集相同.

定义 设 $f(x, y)$ 为二元二次型. n 为非零整数. 如果不定方程 $f(x, y)=n$ 有整数解，则称 f 可以表示 n.

例如：二元二次型 $[1, 0, 1]=x^2+y^2$ 可表示 $1, 2, 4, \cdots$；不可表示 $3, 6, 7, \cdots$. 显然，正定二元二次型只能表示正整数.

我们用 $M(f)$ 表示可以用二元二次型 f 表示的所有非零整数所构成的集合. 例如对 $f=x^2+y^2$，则集合 $M(f)$ 由定理 2 所完全刻划.

引理 4 若 $f\sim g$，则 $M(f)=M(g)$. 换句话说，彼此等价的二元二次型可表示同样的一些非零整数. 即集合 $M(f)$ 是 f 所在的等价类的不变量.

证明 设 $f=[a, b, c]$，$g=[a', b', c']$. 由 $f\sim g$ 可知存在整数 P, Q, R, T，$PT-QR=1$，使得 $g(x, y)=f(Px+Qy, Rx+Ty)$. 如果 g 表示非零整数 n，即 $n\in M(g)$，则有整数 a, b，使得 $g(a, b)=n$. 于是 $f(Pa+Qb, Ra+Tb)=n$，即 f 可表示 n，所以 $n\in M(f)$. 但是由 $f\sim g$ 得到 $g\sim f$. 从而由上面所证即知若 $m\in M(f)$，则 $m\in M(g)$. 这就表明 $M(f)=M(g)$. 证毕.

引理 4 无疑是很重要的. 因为设 $f\sim g$，并且 $g(x, y)=f(Px+Qy, Rx+Ty)$，其中 P, Q, R, T 为整数，并且 $PT-QR=1$. 如果 $g(x, y)=n$ 有整数解，则 $f(x, y)=n$ 也有整数解，且反之亦对. 进而，如果 $(x, y)=(a, b)$ 是 $g(x, y)=n$

的一组整数解，则 $f(Pa+Qb,\ Ra+Tb)=g(a,\ b)=n$，即 $(x,\ y)=(Pa+Qb,\ Ra+Tb)$ 是不定方程 $f(x,\ y)=n$ 的一组整数解．反之，由 $f(x,\ y)=n$ 的一组整数解利用反变换便可得到 $g(x,\ y)=n$ 的一组整数解．总之，只要对于二元二次型 $f(x,\ y)$ 研究方程 $f(x,\ y)=n$ 的整数解，那么同时也就研究了和 f 等价的所有二元二次型的同样问题．这种把某种研究对象（这里是二元二次型）按照某种办法（这里是等价）进行分类，是数学中经常使用的想法．除了研究每类有哪些公共性质之外，另一个想法是希望每个等价类中选举出一个“代表”来．今后我们只需要正定的二元二次型，所以只谈正定二元二次型等价类中如何选代表．

定义 正定二元二次型 $[a,\ b,\ c]$ 叫作标准的，是指它满足如下两个条件：

（I） $|b|\leqslant a\leqslant c$；

（II） 如果 $a=|b|$ 或者 $a=c$，则 $b\geqslant 0$．

定理 5（高斯，正定二元二次型的分类） 每个正定二元二次型均恰好等价于一个标准的正定二元二次型（换句话说，所有标准的正定二元二次型全体恰好组成所有正定二元二次型等价类的代表）．

证明 先证每个正定二元二次型 $f=[M,\ N,\ S]$ 均等价于一个标准的二元二次型．由于 $f(1,\ 0)=M>0$，可知 f 至少可表示一个正整数．我们令 a 为 f 可表示的正整数中最小者，则有整数 A 和 C 使得 $f(A,\ C)=a$．如果 A 和 C 有公因子 l，则 $f\left(\frac{A}{l},\ \frac{C}{l}\right)=\frac{a}{l^2}$ 为正整数．由 a 的最小性知 $|l|=1$，所以 A 和 C 互素．于是有整数 B 和 D，使得 $AD-BC=1$（见附录），

令 $\quad g(x,\ y)=f(Ax+By,\ Cx+Dy)=[a',\ b',\ c']$.

则 $\quad a'=g(1,\ 0)=f(A,\ C)=a$.

这就证明 f 等价于某个二元二次型 $g=[a,\ b',\ c']$.

进而，由前面例 2 可知，对任意整数 m, g(从而 f)等价于 $h(x,\ y)=g(x+my,\ y)=[a,\ 2am+b',\ am^2+b'm+c']$. 我们总可取适当整数 m_0, 使 $b=2am_0+b'$ 满足 $|b|\leqslant a$ (为什么?). 于是 $f\sim[a,\ b,\ c]$, 其中 $c=am_0^2+b'm_0+c'$. 由于 $f(0,1)=c$, 即 f 表示 c. 由 a 的最小性知 $a\leqslant c$. 这就证明了 a, b, c 满足条件(I).

进而若 $a=|b|$, $b<0$, 则 $b=-a$, 而

$$\begin{aligned}f\sim[a,\ b,\ c]=[a,\ -a,\ c]\sim & a(x+y)^2 \\ & -a(x+y)y+cy^2 \\ & =ax^2+axy+cy^2=[a,\ a,\ c],\end{aligned}$$

从而使 $b=a>0$. 最后，若 $a=c$ 而 $b<0$, 则由例 1 知

$$\begin{aligned}f\sim[a,\ b,\ a]=[a,\ b,\ c]\sim[c,\ -b,\ a] \\ =[a,\ -b,\ a].\end{aligned}$$

又使 $-b>0$. 从而又满足条件(II).

再证每个等价类中只有一个标准的二元二次型. 这只需证明：不同的标准正定二元二次型不等价. 设 $f=[a,\ b,\ c]$ 和 $g=[a',\ b',\ c']$ 是两个等价的标准正定二元二次型. 我们要证 $a=a'$, $b=b'$ 和 $c=c'$.

首先有 $f(1,0)=a$, 而当 x 和 y 是不为零的整数时, $f(0,y)=cy^2\geqslant c\geqslant a$, $f(x,\ 0)=ax^2\geqslant a$,

$$\begin{aligned}f(x,\ y)&=ax^2+bxy+cy^2\geqslant ax^2+cy^2-|b|\left(\frac{x^2+y^2}{2}\right) \\ &=\left(a-\frac{|b|}{2}\right)x^2+\left(c-\frac{|b|}{2}\right)y^2\geqslant\frac{a}{2}+\frac{c}{2}\geqslant a.\end{aligned} \tag{10}$$

这表明 a 是 $M(f)$ 中最小正整数. 同样地, a' 是 $M(g)=$

$M(f)$中最小正整数. 于是 $a=a'$. 由于 $f\sim g$, 可知有整数 $A, B, C, D, AD-BC=1$, 使得(见 ⑧ 式)

$$a=a'=aA^2+bAC+cC^2, \tag{11}$$

$$b'=2aAB+b(AD+BC)+2cCD, \tag{12}$$

$$c'=aB^2+bBD+cD^2. \tag{13}$$

由条件(I)知 $a\leqslant c$. 如果 $a<c$, 则由类似于 ⑩ 式的估计可知必然 $C=0$, $A=\pm1$. 再由 $1=AD-BC=AD$ 知 $D=A$. 于是由 ⑬ 式给出 $b'=\pm2aB+b$. 由于 $|b|\leqslant a$, $|b'|\leqslant a'=a$, 可知当 $|b|<a$ 时必然 $b'=b$. 而当 $|b|=a$ 时必然也有 $|b'|=a$. 但这时由条件(II)要求 b', $b>0$, 从而必然 $B=0$, 即 $b'=b$. 从而恒有 $b'=b$. 再由 $b^2-4ac=d=d'=b'^2-4a'c'=b^2-4ac'$ 得到 $c=c'$. 由对称性知若 $a'<c'$, 则同样有 $b=b'$, $c=c'$. 如果 $a=c$, 并且 $a'=c'=a$, 则由条件(II)知 $b>0$, $b'>0$. 于是由 ⑪ 式,

$$a=a(A^2+C^2)+bAC=\frac{a}{2}(A^2+C^2)$$

$$+\left(\frac{a}{2}-\frac{b}{2}\right)(A^2+C^2)+\frac{b}{2}(A+C)^2.$$

于是 $|A|$, $|C|\leqslant1$. 同样用 ⑬ 式可知 $|B|$, $|D|\leqslant1$. 由 $1=AD-BC$ 可知 A, B, C, D 中必有一个为 0. 然后再由 ⑬ 式即可像前面一样证得 $b=b'$, $c=c'$. 这就证明了定理 5.

定理 5 的一个重要推论是:

系 对每个负整数 d, 判别式为 d 的正定二元二次型等价类只有有限个.

证明 由于每个等价类中恰好有一个标准的正定二元二次型, 我们只需证明判别式为 d 的标准正定二元二次型 $[a, b, c]$ 只有有限个. 由条件 (I) 可知

$$4a^2 \leqslant 4ac = -d + b^2 \leqslant -d + a^2,$$

因此 $1 \leqslant a \leqslant \sqrt{\frac{-d}{3}}$. 从而对每个固定的负整数 d, a 只有有限多种取法. 由于 $|b| \leqslant a$, 从而 b 也只有有限多种取法. 最后由 a, b 完全决定 $c = \frac{b^2-d}{4a}$. 这就证明了判别式为 d 的标准正定二元二次型只有有限多个. 证毕.

对每个负整数 d, 我们以 $h(d)$ 表示判别式为 d 的正定二元二次型等价类数, 它也是判别式为 d 的标准正定二元二次型个数. 上面系的证明过程实际上给出了求所有判别式为 d 的标准正定二元二次型的具体方法, 从而决定出 $h(d)$ 值.

【例 3】 $d=-23$. 由 $1 \leqslant a \leqslant \sqrt{\frac{-d}{3}} = \sqrt{\frac{23}{3}}$, 可知 $a=1$ 或 2. 当 $a=1$ 时, $b^2-4ac=-23$, 从而 $4c=b^2+23$, 而 $|b| \leqslant a=1$. 于是 $b=1$, 而 $c=6$. 当 $a=2$ 时, $8c=b^2+23$, 而 $|b| \leqslant a=2$. 于是 $b=\pm 1$ 而 $c=3$. 从而判别式为 -23 的标准正定二元二次型只有三个: $[a, b, c]=[1, 1, 6]$, $[2, 1, 3]$ 和 $[2, -1, 3]$. 于是 $h(-23)=3$.

【例 4】 $d=-4$. 由 $1 \leqslant a \leqslant \sqrt{\frac{4}{3}}$ 可知 $a=1$. 而 $b^2-4c=-4$, $|b| \leqslant 1$. 从而只能 $b=0$, $c=1$. 即判别式为 -4 的正定二元二次型只有一类, 代表为 $x^2+y^2=[1, 0, 1]$, 从而 $h(-4)=1$.

由于 $d=b^2-4ac \equiv b^2 \pmod 4$, 可知二元二次型的判别式模 4 只能余 1 或余 0.

练习 求出判别式为 $d=-3, -7, -8, -11, -12, -15, -16$ 的所有标准正定二元二次型. 并由此决定出 $h(d)$ (对上述 d 值).

4. 三 平 方 和

哪些正整数可表成三平方和，其答案也是很简单的. 这个答案也是很早以前就有人猜测到了，而第一个证明同样是由高斯给出的.

定理6 正整数 n 不为三平方和的充分必要条件是 n 可表为 $4^a(8b+7)$ 的形式，其中 a 和 b 为任意非负整数.

证明 这个定理的一方面是容易证明的：设 $n=4^a(8b+7)$ 为三平方和，即 $n=x^2+y^2+z^2$，其中 x, y, z 均是整数. 如果 $a\geqslant 1$，则 $x^2+y^2+z^2=n\equiv 0 \pmod 4$. 由于奇数平方模 4 余 1，可知若此同余式成立，则 x, y, z 必然均为偶数. 于是

$$4^{a-1}(8b+7)=\frac{n}{4}$$

也可表成三整数平方和 $\left(\frac{x}{2}\right)^2+\left(\frac{y}{2}\right)^2+\left(\frac{z}{2}\right)^2$. 如此继续下去，便知 $8b+7$ 为三平方和：$8b+7=A^2+B^2+C^2$，其中 A, B, C 均为整数. 因此 $A^2+B^2+C^2=8b+7\equiv 7 \pmod 8$. 但是奇数平方模 8 余 1(为什么?)，而偶数平方模 8 余 4 或余 0. 由此易知 $A^2+B^2+C^2\equiv 7 \pmod 8$ 是不可能的. 这就证明了每个形如 $4^a(8b+7)$ 的正整数均不是三平方和.

另一方面，我们要证：所有不能写成 $4^a(8b+7)$ 形式的正整数均是三平方和. 设 n 是这样的正整数. 则我们总可写成 $n=m^2\cdot m'$，其中 m' 是 n 的无平方因子部分. 由于奇数平方模 8 余 1，易知若 n 不能写成 $4^a(8b+7)$ 形式，则 m' 也是如此. 并且只需证明 m' 为三平方和就可以了. 所以我们可以一开始就假定 n 本身没有平方因子. 换句话说，我们将问题归结为证明：

命题 设 n 是不同素数的乘积，并且 $n\neq 7 \pmod 8$，则 n 为三平方和.

为了证明上述命题，除了上节所述关于二元二次型的结果之外，还需要一点三元二次型的知识. 这是因为三平方和表达式 $x^2+y^2+z^2$ 本身是三元二次型.

三元二次型是形如下面的函数

$$f(x, y, z)=a_{11}x^2+a_{22}y^2+a_{33}z^2+a_{12}xy+a_{13}xz+a_{23}yz, \tag{14}$$

其中 a_{ij} 均是整数. 并且行列式

$$d=d(f)=\begin{vmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{vmatrix}$$

$$=8a_{11}a_{22}a_{33}+2a_{12}a_{13}a_{23}-2a_{13}^2a_{22}-2a_{12}^2a_{33}-2a_{23}^2a_{11}$$

的值叫作 f 的判别式. 如果 $f(x, y, z)$ 只表示正整数，即对任何不全为零的整数 x, y, z，均有 $f(x, y, z)>0$，则称 f 是正定的. 例如 $x^2+y^2+z^2$ 就是正定的三元二次型. 下面是三元二次型正定性的判别法.

引理 5 形如 ⑭ 式的三元二次型 $f(x, y, z)$ 为正定的充分必要条件是

$$a_{11}>0,\ b=\begin{vmatrix} 2a_{11} & a_{12} \\ a_{12} & 2a_{22} \end{vmatrix}=4a_{11}a_{22}-a_{12}^2>0,$$

并且 $d=d(f)>0$.

证明 可直接验证

$$f(1, 0, 0)=a_{11},\ f(x, y, 0)=a_{11}x^2+a_{12}xy+a_{22}y^2.$$

若 f 正定，则 $a_{11}>0$，并且 $f(x, y, 0)$ 是关于 x, y 的正定二元二次型. 由上节可知它的判别式 $a_{12}^2-a_{11}a_{22}=-b<0$，即 $b>0$. 进而，我们有

$$4a_{11}f(x, y, z)=(2a_{11}x+a_{12}y+a_{13}z)^2+g(y, z), \qquad ⑮$$

其中 $$g(y, z)=(4a_{11}a_{22}-a_{12}^2)y^2+(4a_{11}a_{23}-2a_{12}a_{13})yz+(4a_{11}a_{33}-a_{13}^2)z^2.$$

而 g 的判别式为

$$(4a_{11}a_{23}-2a_{12}a_{13})^2-4(4a_{11}a_{22}-a_{12}^2)(4a_{11}a_{33}-a_{13}^2)=-8a_{11}d(f).$$

如果 f 正定，则 $g(y, z)$ 也正定(这是由于：若 g 不正定，则存在不全为零的整数 B 和 C，使 $g(B, C)\leqslant 0$. 于是由⑮式可知

$$4a_{11}f(-a_{12}B-a_{13}C, 2a_{11}B, 2a_{11}C)=g(2a_{11}B, 2a_{11}C)=4a_{11}^2g(B, C)\leqslant 0.$$

这就与 f 正定相矛盾). 因此 g 的判别式 $-8a_{11}d(f)$ 为负，即 $d(f)>0$.

反之，若 $a_{11}>0$, $b>0$, $d(f)>0$，则 g 是正定的，再由⑮式即知 f 是正定的. 证毕.

可以像二元二次型那样定义三元二次型的等价：

定义 三元二次型 $f(x, y, z)$ 和 $g(x, y, z)$ 等价 (表示为 $f\sim g$)，是指存在整数 $b_{ij}(1\leqslant i, j\leqslant 3)$，使得

$$\begin{vmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{vmatrix}=1,$$

并且 $$g(x, y, z)=f(b_{11}x+b_{12}y+b_{13}z, b_{21}x+b_{22}y+b_{23}z, b_{31}x+b_{32}y+b_{33}z).$$

可以像二元二次型一样地证明，三元二次型的等价也具有自反性、对称性和传递性. 从而三元二次型分成一些等价类，同一等价类中的三元二次型彼此等价，而不同等价类中的

三元二次型彼此不等价. 进而, 彼此等价的正定三元二次型具有同样的判别式, 并且表示同样的整数. 于是正定三元二次型只能与正定三元二次型等价. 如果大家会矩阵运算, 以上结论甚至对任意 n 元二次型都可以统一地给出形式化的证明. 否则, 对于三元二次型也可像前节那样作初等计算来直接验证, 不过比二元二次型的计算要复杂一些. 我们在这里最好略去这些计算, 留给有兴趣的读者自己作为练习. 我们感兴趣的是每个正定三元二次型等价类中如何挑选出"标准"的代表, 下面定理对我们就已经够用了.

定理 7 每个正定三元二次型 f 都等价于一个新的三元二次型, 使得系数满足条件:

$$1 \leqslant a_{11} \leqslant \frac{2}{3}\sqrt[3]{d(f)},\ |a_{12}| \leqslant a_{11},\ |a_{13}| \leqslant a_{11}.$$

证明 设 $f(x, y, z)$ 是正定三元二次型. 以 a_{11} 表示可用 f 表示的最小正整数. 则存在整数 A, B, C, 使得 $f(A, B, C) = a_{11}$. 由 a_{11} 的最小性可知 $(A, B, C) = 1$. 于是有整数 M, N, P, 使得 $AM + BN + CP = 1$(见附录). 设 $(M, N) = l$, 则 $\frac{M}{l}$, $\frac{N}{l}$ 是互素的整数. 从而有整数 Q 和 R 使得

$$\frac{M}{l}Q + \frac{N}{l}R = P.$$

于是

$$\begin{vmatrix} A & B & C \\ -Q & -R & l \\ \frac{N}{l} & -\frac{M}{l} & 0 \end{vmatrix} = AM + BN + C\left(\frac{M}{l}Q + \frac{N}{l}R\right)$$

$$= AM + BN + CP = 1.$$

令 $g(x, y, z)=f\left(Ax-Qy+\frac{N}{l}z,\ Bx-Ry-\frac{M}{l}z,\right.$

$$\left.Cx+ly\right),$$

则 $g\sim f$, 并且 $g(1, 0, 0)=f(A, B, C)=a_{11}$. 即

$$g(x, y, z)=a'_{11}x^2+a'_{22}y^2+a'_{33}z^2+a'_{12}xy+a'_{13}xz+a'_{23}yz,$$

其中 $a'_{11}=a_{11}$. 现设 P, Q 为任意整数, A, B, C, D 为整数, 使得 $AD-BC=1$. 则

$$\begin{vmatrix} 1 & P & Q \\ 0 & A & B \\ 0 & C & D \end{vmatrix}=1,$$

因此令 $h(x, y, z)=g(x+Py+Qz,\ Ay+Bz,\ Cy+Dz)$,

则 $h\sim g\sim f$, 并且 $h(1, 0, 0)=g(1, 0, 0)=a_{11}$. 于是 h 可写成

$$h(x, y, z)=a_{11}x^2+a_{22}y^2+a_{33}z^2+a_{12}xy+a_{13}xz+a_{23}yz,$$

其中

$$a_{12}=2Pa_{11}+Aa'_{12}+Ca'_{13},\quad a_{13}=2Qa_{11}+Ba'_{12}+Da'_{13}. \qquad ⑯$$

像引理 5 的证明中那样我们有

$$4a_{11}h=(2a_{11}x+a_{12}y+a_{13}z)^2+H(y, z),$$

其中 $H(y, z)=(4a_{11}a_{22}-a_{12}^2)y^2+\cdots$. 并且 H 的判别式 $d(H)$ 为 $-8a_{11}d(f)$. 由上节定理 5 的系知道, 适当选取 A, B, C, D, 可使

$$1\leqslant 4a_{11}a_{22}-a_{12}^2\leqslant\sqrt{\frac{-d(H)}{3}}=\sqrt{\frac{8a_{11}d(f)}{3}}.$$

然后对于固定的 A, B, C, D, 由 ⑯ 式知道, 适当选取 P 和 Q 可使 $|a_{12}|\leqslant a_{11}$, $|a_{13}|\leqslant a_{11}$. 再由 $a_{22}=h(0, 1, 0)$ 和 a_{11} 的

最小性知 $a_{22}\geqslant a_{11}$. 于是

$$4a_{11}^2\leqslant 4a_{11}a_{22}=(4a_{11}a_{22}-a_{12}^2)+a_{12}^2\leqslant\sqrt{\frac{8a_{11}d(f)}{3}}+a_{11}^2.$$

由此即知 $a_{11}\leqslant\frac{2}{3}\sqrt[3]{d(f)}$. 证毕.

由这个定理立即得到:

系 设 $f(x, y, z)=a_{11}x^2+a_{22}y^2+a_{33}z^2+a_{12}xy+a_{13}xz+a_{23}yz$ 是正定三元二次型, 判别式 $d(f)=8$, 并且 a_{12}, a_{13}, a_{23} 均是偶数,则 f 必等价于 $x^2+y^2+z^2$.

证明 如果 f 中系数 a_{12}, a_{13}, a_{23} 均为偶数, 易知与 f 等价的每个三元二次型也有这个性质. 根据定理 7 知 f 等价于 $h=b_{11}x^2+b_{22}y^2+b_{33}z^2+b_{12}xy+b_{13}xz+b_{23}yz$, 并且

$$1\leqslant b_{11}\leqslant\frac{2}{3}\sqrt[3]{8}=\frac{4}{3}.$$

于是 $b_{11}=1$. 而 $|b_{12}|\leqslant1$, $|b_{13}|\leqslant1$. 由于 b_{12} 和 b_{13} 均为偶数, 从而 $b_{12}=b_{13}=0$. 因此 $h=x^2+b_{22}y^2+b_{23}yz+b_{33}z^2=x^2+H(y, z)$, 其中 H 的判别式为 $d(H)=b_{23}^2-4b_{22}b_{33}$. 但是

$$8=d(f)=d(h)=\begin{vmatrix}2 & 0 & 0\\ 0 & 2b_{22} & b_{23}\\ 0 & b_{23} & 2b_{33}\end{vmatrix}=-2d(H),$$

因此 $d(H)=-4$. 上小节最后一个例子表明 $H(y,z)\sim y^2+z^2$. 于是 $f\sim h\sim x^2+y^2+z^2$. 证毕.

现在我们回过头来证明我们的三平方和定理. 我们已经把问题归结为证明如下的命题: 设 n 是一些不同素数乘积, 并且 $n\not\equiv7\pmod 8$, 则 n 是三平方和. 我们刚刚证明过, 每个判别式为 8 并且 a_{12}, a_{13}, a_{23} 均为偶数的正定三元二次型均等价于三平方和. 所以我们只需找到一个这样的三元二次型, 使得它能够表示 n 即可 (因为这表明与它等价的 $x^2+y^2+z^2$

也表示 n). 事实上,我们试图构作如下形式的三元二次型:

$$f(x, y, z)=a_{11}x^2+2a_{12}xy+2xz+a_{22}y^2+nz^2.$$

这样的三元二次型显然表示 n: $f(0, 0, 1)=n$. 我们要求它的判别式为 8, 即要求

$$8=\begin{vmatrix} 2a_{11} & 2a_{12} & 2 \\ 2a_{12} & 2a_{22} & 0 \\ 2 & 0 & 2n \end{vmatrix}=8[(a_{11}a_{22}-a_{12}^2)n-a_{22}],$$

即要求 $nb-a_{22}=1$, 其中 $b=a_{11}a_{22}-a_{12}^2$. 此外还要求 f 正定, 即要求 $a_{11}>0$, $b>0$. 不妨设 $n\geqslant 2$. 这时由 $nb-a_{22}=1$ 和 $b>0$ 可推出 $a_{11}>0$(因为 $a_{22}=nb-1>0$, $a_{11}a_{22}=a_{12}^2+b>0$, 从而 $a_{11}>0$). 因此我们将问题化为如下的形式:

设 n 是不同素数之乘积并且 $n\not\equiv 7 \pmod 8$. 求整数 a_{11}, a_{22}, a_{12}, 使得 $b=a_{11}a_{22}-a_{12}^2>0$, $nb-a_{22}=1$.

由对 n 的限制知 $n\equiv 1, 2, 3, 5, 6 \pmod 8$. 我们分两种情形:

(i) 设 n 为偶数, 即 $n\equiv 2, 6 \pmod 8$, 则 $(4n, n-1)=1$. 根据狄里赫利算术级数中素数定理(见附录), 存在正整数 m, 使得 $4nm+(n-1)=p$ 为素数. 我们取 $b=4m+1$, 则 $p=bn-1$, 并且 $b\equiv p\equiv 1 \pmod 4$. 设 $b=p_1\cdots p_s$, 其中 $p_1, \cdots, p_s$ 均为奇素数. 则由二次互反律可知(见附录)

$$\left(\frac{-b}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{p_1}{p}\right)\cdots\left(\frac{p_s}{p}\right)=\left(\frac{p}{p_1}\right)\cdots\left(\frac{p}{p_s}\right).$$

但是 $\qquad p=bn-1=p_1\cdots p_s n-1\equiv -1 \pmod{p_i}$,

因此 $$\left(\frac{p}{p_i}\right)=\left(\frac{-1}{p_i}\right) \quad (1\leqslant i\leqslant s).$$

于是 $$\left(\frac{-b}{p}\right)=\left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_s}\right).$$

由于 $b=p_1\cdots p_s\equiv 1 \pmod 4$, 可知 $p_i(1\leqslant i\leqslant s)$ 中模 4 余 3 的

必有偶数个．因此$\left(\frac{-b}{p}\right)=\left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_s}\right)=1$．这表明$-b$是$p$的二次剩余．于是存在整数$a_{12}$，使得$a_{12}^2\equiv-b\pmod p$．再令$a_{22}=bn-1=p>0$，$a_{11}=\frac{b+a_{12}^2}{a_{22}}=\frac{b+a_{12}^2}{p}$，则$a_{11}$为整数．这样决定的$a_{11}$，$a_{22}$和$a_{12}$满足我们的要求．

（ii）设n为奇数，则$n\equiv1, 3, 5\pmod 8$．令

$$c=\begin{cases}3, & 若\ n\equiv1\pmod 8,\\ 1, & 若\ n\equiv3\pmod 8,\\ 3, & 若\ n\equiv5\pmod 8,\end{cases}$$

则$cn-1\equiv2\pmod 4$．于是$\left(4n, \frac{cn-1}{2}\right)=1$．从而存在正整数$m$，使得$4nm+\frac{cn-1}{2}=p$为奇素数．现在令$b=8m+c$，则$2p=bn-1$．现在我们证明$\left(\frac{-b}{p}\right)=1$．例如当$n\equiv1\pmod 8$时，$b\equiv c\equiv3\pmod 8$，$p\equiv\frac{3n-1}{2}\equiv1\pmod 4$．令$b=p_1\cdots p_s$，其中$p_1, \cdots, p_s$均为奇素数，则

$$\left(\frac{-b}{p}\right)=\left(\frac{b}{p}\right)=\left(\frac{p_1}{p}\right)\cdots\left(\frac{p_s}{p}\right)=\left(\frac{p}{p_1}\right)\cdots\left(\frac{p}{p_s}\right)$$
$$=\left(\frac{2}{p_1}\right)\cdots\left(\frac{2}{p_s}\right)\left(\frac{2p}{p_1}\right)\cdots\left(\frac{2p}{p_s}\right).$$

由于$2p=bn-1=p_1\cdots p_sn-1\equiv-1\pmod{p_i}\ (1\leqslant i\leqslant s)$，因此$\left(\frac{-b}{p}\right)=\left(\frac{-2}{p_1}\right)\cdots\left(\frac{-2}{p_s}\right)$．由于$b=p_1\cdots p_s\equiv3\pmod 8$，并且

$$\left(\frac{-2}{p}\right)=\begin{cases}1, & 当\ p\equiv1, 3\pmod 8\ 时,\\ -1, & 当\ p\equiv5, 7\pmod 8\ 时,\end{cases}$$

可知$p_i\ (1\leqslant i\leqslant s)$中模8同余于5和7的共有偶数个．因此$\left(\frac{-b}{p}\right)=1$．对于$n\equiv3, 5\pmod 8$的情形可以类似证明．于

是存在整数 a_{12}，使 $a_{12}^2\equiv-b \pmod p$．由于 p 是奇素数，必要时将 a_{12} 改用 $a_{12}+p$，可以设 a_{12} 为奇数．从而 $a_{12}^2\equiv-b \pmod{2p}$．令 $a_{22}=bn-1=2p$，则 $a_{11}=\frac{(a_{12}^2+b)}{a_{22}}=\frac{a_{12}^2+b}{2p}$ 为整数，于是 a_{11}，a_{12}，a_{22} 满足我们的条件．

这样，我们终于完成了三平方和定理的证明．

最后我们再谈谈三平方和表示 n 的表法个数问题．高斯第一个给出了与二元二次型等价类数有关的表法公式．它的证明则需要更高深的数论．在这本小册子里我们不想介绍证明本身，而只叙述其结果，算作是一个交待．

设 m 为正整数．不定方程

$$m=x^2+y^2+z^2$$

的整数解 (x, y, z) 叫作是*本原的*，是指 x, y, z 的最大公因子为 1．我们前面曾经用 $r_3(m)$ 表示上面不定方程的整解个数，它也是 m 表成三平方和的表法个数．现在我们再以 $R_3(m)$ 表示上面不定方程的本原整解个数．对于上述方程的任意一组整解 $(x, y, z)=(a, b, c)$，若 d 为 a, b, c 的最大公因子，则 $\frac{a}{d}, \frac{b}{d}, \frac{c}{d}$ 的最大公因子为 1，并且 $\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right)$ 是不定方程

$$\frac{m}{d^2}=x^2+y^2+z^2$$

的一组本原整解．因此便知

$$r_3(m)=\sum_{d^2\mid m} R_3\left(\frac{m}{d^2}\right).$$

其中 d^2 过 m 的所有平方因子．特别当 m 无平方因子时，

$$r_3(m)=R_3(m).$$

另一方面，我们曾经用 $h(-m)$ 表示判别式为 $-m$ 的正

定二元二次型等价类数. 二元二次型 $ax^2+bxy+cy^2$ 叫作本原的, 是指$(a, b, c)=1$(即 a, b, c 的最大公因子为1). 易知本原的二元二次型只能与本原二元二次型等价. 我们用 $H(-m)$表示判别式为 $-m$ 的本原二元二次型等价类数. 则类似地也有

$$h(-m)=\sum_{d^2\mid m}H\left(-\frac{m}{d^2}\right).$$

特别当m无平方因子时, $h(-m)=H(-m)$.

高斯定理 设 $m\geqslant 2$. 则

$$R_3(m)=\begin{cases}12H(-m), & \text{若 } m\not\equiv 3 \pmod 8,\\ 8H(-m), & \text{若 } m\equiv 3 \pmod 8.\end{cases}$$

而 $R_3(1)=6$.

二、再谈整数平方和
——有多少种表示法?

设 k 为正整数. 对每个正整数 n, 以 $r_k(n)$ 表示用 k 个整数的平方和表示 n 的表法个数, 它也等于不定方程 $x_1^2+x_2^2+\cdots+x_k^2=n$ 的整数解 $(x_1, x_2, \cdots, x_k)$ 的个数. 我们在上一节解决了何时 $r_k(n)\geqslant 1$ 的问题. 例如, 拉格朗日定理是说, 当 $k\geqslant 4$ 时, 对每个正整数 n, 均有 $r_k(n)\geqslant 1$. 本节谈 $r_k(n)$ 的计算公式问题. 我们将要推导 $r_2(n)$ 和 $r_4(n)$ 的表达式. 我们也要谈到对其他 k 值的 $r_k(n)$ 公式, 而 $r_3(n)$ 在上一节已经介绍了.

研究计数问题的常见办法是以母函数作为工具. 目前国内已有许多种介绍母函数方法的参考书籍. 但是, 平方和问题所使用的母函数却很不简单. 系统地研究这类母函数的特性, 则是数论的一个分支——模形式理论的一个重要任务. 这个分支近年来得到巨大的发展, 其动力之一就是希望系统地得出 $r_k(n)$ (特别当 k 为奇数时) 的计算公式并研究整数 $r_k(n)$ 的各种特性(渐近性质, 同余性质等等). 我们不准备涉及很高深的学问, 本书中只用很初等的方法利用母函数计算出 $r_2(n)$ 和 $r_4(n)$ 的公式. 最后, 我们还介绍高斯给出的关于 $r_2(n)$ 公式的一个代数证明, 因为这个证明在数论史上是有重要地位的, 它的思想直接引伸出数论的另一个分支——代数数论.

让我们从 $r_k(n)$ 的母函数和与此有关的另一些重要函数讲起.

1. θ, q_0, q_1, q_2 和 q_3

凡是了解母函数方法的人,都很容易理解以下事实:

设
$$\theta(x)=\sum_{m=-\infty}^{\infty} x^{m^2}=1+2\sum_{m=1}^{\infty} x^{m^2}$$
$$=1+2(x+x^4+x^9+x^{16}+\cdots),$$
那么 $\theta(x)$ 中 x^n 的系数恰好等于方程 $z^2=n$ 的整数解个数,因为当 $n=0$ 时 $z^2=0$ 只有一个整数解 $z=0$,而当 n 是非零平方数 m^2 时,$z^2=m^2$ 有两个整数解 $z=\pm m$. 进而,我们将 $\theta(x)$ 乘以 $\theta(x)$ 再合并同类项:
$$\theta^2(x)=\left(\sum_{m=-\infty}^{\infty} x^{m^2}\right)\left(\sum_{r=-\infty}^{\infty} x^{r^2}\right)=\sum_{m,r=-\infty}^{\infty} x^{m^2+r^2}$$
将所有 m^2+r^2 相同的收集在一起,对于每个正整数 n,使 m^2+r^2 等于 n 的项数恰好是方程 $z_1^2+z_2^2=n$ 的整解个数 $r_2(n)$. 由于每项的系数均是 1,所以 $\theta^2(x)$ 中 x^n 项的系数恰好是 $r_2(n)$. 即
$$\theta^2(x)=1+\sum_{n=1}^{\infty}\sum_{\substack{m,r=-\infty\\ m^2+r^2=n}}^{\infty} x^{m^2+r^2}=1+\sum_{n=1}^{\infty}\sum_{\substack{m,r=-\infty\\ m^2+r^2=n}}^{\infty} x^n$$
$$=1+\sum_{n=1}^{\infty} r_2(n)x^n.$$
换句话说,$\theta^2(x)$ 恰好是 $r_2(n)$ 的母函数. 类似地思考,可知对每个正整数 k,$\theta^k(x)$ 恰好是 $r_k(n)$ 的母函数,即
$$\theta^k(x)=1+\sum_{n=1}^{\infty} r_k(n)x^n.$$
于是,$r_k(n)$ 的母函数便这样容易地找到了.为了研究 $r_k(n)$ 的

特性，需要考察函数 $\theta(x)$ 和它的各种方幂的特性． 这却是一件相当困难的事情． 函数 $\theta(x)$ 叫作 theta 函数，它与另外几个有同样大名气的函数有密切关系．这些函数是

$$
\begin{aligned}
q_0=q_0(x)&=\prod_{m=1}^{\infty}(1-x^{2m})\\
&=(1-x^2)(1-x^4)(1-x^6)(1-x^8)(1-x^{10})\cdots\\
&=1-x^2-x^4+x^{10}+\cdots,
\end{aligned}
$$

$$
\begin{aligned}
q_1=q_1(x)&=\prod_{m=1}^{\infty}(1+x^{2m})\\
&=(1+x^2)(1+x^4)(1+x^6)(1+x^8)(1+x^{10})\cdots\\
&=1+x^2+x^4+2x^6+2x^8+3x^{10}+\cdots,
\end{aligned}
$$

$$
\begin{aligned}
q_2=q_2(x)&=\prod_{m=1}^{\infty}(1+x^{2m-1})\\
&=(1+x)(1+x^3)(1+x^5)(1+x^7)(1+x^9)+\cdots\\
&=1+x+x^3+x^4+x^5+x^6+x^7\\
&\quad+2x^8+2x^9+2x^{10}+\cdots,
\end{aligned}
$$

$$
\begin{aligned}
q_3=q_3(x)&=\prod_{m=1}^{\infty}(1-x^{2m-1})\\
&=(1-x)(1-x^3)(1-x^5)(1-x^7)(1-x^9)\cdots\\
&=1-x-x^3+x^4-x^5+x^6-x^7\\
&\quad+2x^8-2x^9+2x^{10}+\cdots.
\end{aligned}
$$

这几个函数叫作椭圆模函数，我们不想解释这个名称的来由，因为它具有深刻的数学背景． 我们只希望大家"形式"上理解它们：虽然它们都是用无穷多个因式相乘定义的，但是在将它们按 x 的升幂次写成展开式时，对于每个正整数 n，x^n 的系数只由前面有限个因式相乘就完全确定． 我们以 q_0 为例，如果求 q_0 展开式中 x^8 的系数，那么它等于

$$A=(1-x^2)(1-x^4)(1-x^6)=1-x^2-x^4+x^8+x^{10}-x^{12}$$

中 x^6 的系数(即为0). 因为如果再乘下一个因式 $(1-x^8)$, 则 $A(1-x^8)=A-x^8A$, 由于 x^8A 中每项 x 的指数均大于8, 从而对 x^6 的系数没有贡献. 即 $A(1-x^8)=(1-x^2)(1-x^4)(1-x^6)(1-x^8)$ 中 x^6 的系数仍旧为零. 正是在这种意义下, 可以将无穷乘积 $\prod_{m=1}^{\infty}(1-x^{2m})$ 展开成 $1+a_1x+a_2x^2+\cdots$(或者说成是关于 x 的"形式幂级数")对于 q_1, q_2, q_3 情形也是类似的.

函数 θ^k 的展开式系数 $r_k(n)$ 具有"k 平方和"这一数论意义. 那么函数 q_0, q_1, q_2, q_3(和它们的组合)的展开式系数是否也有数论意义呢? 答案是肯定的; 这些函数与正整数的分拆问题有密切关系.

把正整数 n 写成若干正整数之和, 叫作 n 的一个分拆. 如数5共有以下七种分拆方法:

$$5=4+1=3+2=3+1+1=2+2+1=2+1+1+1$$
$$=1+1+1+1+1.$$

其中 $4+1$ 和 $1+4$ 看成是同样的分拆, 通常以 $p(n)$ 表示 n 的分拆方法数. 如 $p(5)=7$.

现在我们考察无穷乘积

$$q_1=\prod_{m=1}^{\infty}(1+x^{2m})$$
$$=(1+x^2)(1+x^4)(1+x^6)(1+x^8)(1+x^{10})\cdots.$$

从右边有限多个因子中取出它们的第二项, 而其余因子均取第一项1, 乘起来便得到 q_1 展开式中的一个单项式. 例如将第一、三、五个因子分别取第二项 x^2、x^6 和 x^{10}, 而其余因子均取第一项1, 相乘得出 q_1 的一个单项式 $x^2\cdot x^6\cdot x^{10}=x^{2+6+10}=x^{18}$. q_1 中所有单项式都是这样得到的. 如果再将它们合并同类项,

比如说共有多少项是 x^{18}，就看有多少种取法，使每次所取因子第二项 x 指数之和为 18，易知共有 18，2+16，4+14，6+12，8+10，2+4+12，2+6+10，4+6+8 这八种取法，于是合并同类项后 q_1 的展开式中有 $8x^{18}$ 这一项．由于无穷乘积中所有因子第二项的指数恰好是全部偶数，因此对每个整数 n，展开式中单项式 x^n 的个数恰好是将 n 分拆成一些彼此不同的正偶数之和的方法数．如果将此数表示成 $p_0'(n)$，则在合并同类项后 q_1 的展开式中便有 $p_0'(n)x^n$ 这一项．于是

$$q_1=1+\sum_{n=1}^{\infty} p_0'(n)x^n.$$

即 q_1 是 $p_0'(n)$ 的母函数．类似地，若以 $p_1'(n)$ 表示将 n 分拆成一些彼此不同的正奇数之和的方法数，则 q_2 是 $p_1'(n)$ 的母函数，即

$$q_2=\prod_{m=1}^{\infty}(1+x^{2m-1})=1+\sum_{n=1}^{\infty} p_1'(n)x^n.$$

而 $$q_1q_2=\prod_{m=1}^{\infty}(1+x^{2m-1})(1+x^{2m})=\prod_{m=1}^{\infty}(1+x^m)$$

(所有正偶数指数与正奇数指数恰好合并成所有正整数指数．)

$$=(1+x)(1+x^2)(1+x^3)(1+x^4)\cdots$$

$$=1+\sum_{n=1}^{\infty} p'(n)x^n,$$

其中 $p'(n)$ 表示 n 分拆成一些不同正整数之和的方法数．再看

$$q_0^{-1}=\prod_{m=1}^{\infty}(1-x^{2m})^{-1}$$

$$=\prod_{m=1}^{\infty}(1+x^{2m}+x^{2(2m)}+x^{3(2m)}+x^{4(2m)}+\cdots)$$

$$=(1+x^2+x^{2\cdot 2}+x^{3\cdot 2}+\cdots)(1+x^4+x^{2\cdot 4}+x^{3\cdot 4}+\cdots)$$

$$(1+x^6+x^{2\cdot 6}+x^{3\cdot 6}+\cdots)(1+x^8+x^{2\cdot 8}+x^{3\cdot 8}+\cdots).$$

如果我们从第一、二、四个括号中分别取 $x^{3\cdot 2}$、$x^{2\cdot 4}$ 和 x^8，而其余括号均取第一项 1，便得到 q_0^{-1} 展开式中的一个单项式 $x^{3\cdot 2+2\cdot 4+1\cdot 8}=x^{22}$. 我们将它看成是将 22 分拆成 3 个 2，2 个 4 和 1 个 8 之和：$22=2+2+2+4+4+8$，即此处分拆允许有相同分量. 于是，合并同类项之后，q_0^{-1} 展开式中 x^n 的系数便等于将 n 分拆成一些正偶数（允许相同）之和的方法数，记它为 $p_0(n)$，则 q_0^{-1} 为 $p_0(n)$ 的母函数：

$$q_0^{-1}=1+\sum_{n=1}^{\infty} p_0(n)x^n.$$

类似地，q_3^{-1} 为 $p_1(n)$ 的母函数，其中 $p_1(n)$ 为将 n 分拆成一些正奇数之和的方法数，即

$$q_3^{-1}=\prod_{m=1}^{\infty}(1-x^{2m-1})^{-1}=1+\sum_{n=1}^{\infty} p_1(n)x^n.$$

最后
$$(q_0q_3)^{-1}=\prod_{m=1}^{\infty}(1-x^{2m-1})^{-1}(1-x^{2m})^{-1}$$
$$=\prod_{m=1}^{\infty}(1-x^m)^{-1}=1+\sum_{n=1}^{\infty} p(n)x^n,$$

其中 $p(n)$ 恰好就是我们最早定义的 n 的分拆数，它的母函数为 $(q_0q_3)^{-1}$.

设 $a(n)$ 是具有数论（或其他数学）意义的值. 一旦我们求得它的母函数 $f(x)=\sum_{n=0}^{\infty} a(n)x^n$，我们可以暂时忘掉 $a(n)$ 的数学意义，而对 $f(x)$ 作形式推导，发现 $f(x)$ 的性质或与其他母函数之间的联系，然后回到原始数学意义中，便会得到许多有趣的数学结论. 现在我们研究函数 q_0, q_1, q_2, q_3 以及 θ 的性质和联系. 首先我们有

引理 1 $q_1q_2q_3=1$.

证明 由于 $q_1=\prod_{m=1}^{\infty}(1+x^{2m})$，而每个偶数 $2m$ 均可唯一

地写成形式 $2m=2^a(2b-1)$，其中 a, b 均为正整数. 于是

$$q_1=\prod_{b=1}^{\infty}(1+x^{2(2b-1)})\prod_{b=1}^{\infty}(1+x^{4(2b-1)})$$

$$\times\prod_{b=1}^{\infty}(1+x^{8(2b-1)})\cdots.$$

从而

$$q_1q_2q_3=\left(\prod_{m=1}^{\infty}(1+x^{2m-1})(1-x^{2m-1})\right)\cdot q_1$$

$$=\prod_{b=1}^{\infty}(1-x^{2(2b-1)})\prod_{b=1}^{\infty}(1+x^{2(2b-1)})$$

$$\times\prod_{b=1}^{\infty}(1+x^{4(2b-1)})\cdots$$

$$=\prod_{b=1}^{\infty}(1-x^{4(2b-1)})\prod_{b=1}^{\infty}(1+x^{4(2b-1)})$$

$$\times\prod_{b=1}^{\infty}(1+x^{8(2b-1)})\cdots$$

$$=\prod_{b=1}^{\infty}(1-x^{8(2b-1)})\prod_{b=1}^{\infty}(1+x^{8(2b-1)})$$

$$\times\prod_{b=1}^{\infty}(1+x^{16(2b-1)})\cdots=\cdots.$$

于是这样下去，$q_1q_2q_3$ 的展开式中除了 1 之外，所有其他项均不存在. 因此 $q_1q_2q_3=1$. 证毕.

引理 1 也可写成 $(q_3)^{-1}=q_1q_2$. 但是左边和右边分别是 $p_1(n)$ 和 $p'(n)$ 的母函数(回到数论意义). 这就证明了：将正整数 n 分拆成正奇数之和的方法数等于将 n 分拆成不同正整数之和的方法数.

下节将研究更进一步的恒等式.

2. 雅可比恒等式

雅可比(Jacobi)恒等式具有广泛的应用，由它可得到许

多有趣的恒等式，它也是我们用母函数方法研究平方和表法公式的最基本出发点，因为这个恒等式给出椭圆模函数 q_i 和 θ 之间的联系.

定理1(雅可比恒等式) 对任意 $z\neq 0$，我们有

$$\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1}z)(1+x^{2n-1}z^{-1})$$

$$=1+\sum_{n=1}^{\infty}x^{n^2}(z^n+z^{-n})=\sum_{n=-\infty}^{\infty}x^{n^2}z^n.$$

证明 第二个等式显然成立，我们只需证第一个等式. 令

$$\begin{aligned}\varphi_m(z)=&\prod_{n=1}^{m}(1+x^{2n-1}z)(1+x^{2n-1}z^{-1})\\ =&X_0+X_1(z+z^{-1})+X_2(z^2+z^{-2})\\ &+\cdots+X_m(z^m+z^{-m}),\end{aligned}\qquad ㊅$$

此处，X_0，X_1，…，X_m 为 x 的函数而与 z 无关(由 $\varphi_m(z)=\varphi_m(z^{-1})$ 易知展开式中 z^i 和 z^{-i} 必有相同的系数 X_i). 最高次项 X_mz^m 的系数 X_m 必然是每个因子

$$(1+x^{2n-1}z)(1+x^{2n-1}z^{-1})$$

$$=1+x^{2n-1}z^{-1}+x^{4n-2}+x^{2n-1}z$$

中均取最高次项 $x^{2n-1}z$，然后将它们相乘得到的. 于是

$$X_m=\prod_{n=1}^{m}x^{2n-1}=x^{1+3+5+\cdots+(2m-1)}=x^{m^2}.$$

进而，

$$\begin{aligned}\varphi_m(x^2z)=&\prod_{n=1}^{m}(1+x^{2n+1}z)(1+x^{2n+1}z^{-1})\\ =&\frac{1+x^{-1}z^{-1}}{1+xz}\cdot\frac{1+x^{2m+1}z}{1+x^{2m+1}z^{-1}}\varphi_m(z)\\ =&\frac{1+x^{2m+1}z}{xz+x^{2m}}\varphi_m(z),\end{aligned}$$

即

$$(xz+x^{2m})\varphi_m(x^2z)=(1+x^{2m+1}z)\varphi_m(z).$$

将㊅式代入,并比较 z^{1-n} 的系数，便得到

$$X_n=\frac{x^{2n-1}(1-x^{2m-2n+2})}{1-x^{2m+2n}}\,X_{n-1},$$

由此式迭代下去即得

$$X_n=x^{n^2}\frac{(1-x^{2m-2n+2})(1-x^{2m-2n+4})\cdots(1-x^{2m})}{(1-x^{2m+2n})(1-x^{2m+2n-2})\cdots(1-x^{2m+2})}\,X_0.$$

但是 $X_m=x^{m^2}$, 从而

$$X_0=\frac{(1-x^{4m})(1-x^{4m-2})\cdots(1-x^{2m+2})}{(1-x^2)(1-x^4)\cdots(1-x^{2m})}.$$

于是对 $0\leqslant n\leqslant m-1$ 则有

$$X_n=\frac{x^{n^2}}{(1-x^2)(1-x^4)\cdots(1-x^{2m})}\,X'_n,$$

其中
$$\begin{aligned}X'_n&=\frac{(1-x^{2m-2n+2})(1-x^{2m-2n+4})\cdots(1-x^{2m})}{(1-x^{2m+2n})(1-x^{2m+2n-2})\cdots(1-x^{2m+2})}\\&\quad\times(1-x^{2m+2})(1-x^{2m+4})\cdots(1-x^{4m})\\&=(1-x^{2m-2n+2})(1-x^{2m-2n+4})\cdots(1-x^{2m})\\&\quad\times(1-x^{2m+2n+2})(1-x^{2m+2n+4})\cdots(1-x^{4m}).\end{aligned}$$

从而㊀式可写成

$$\begin{aligned}&(1-x^2)(1-x^4)\cdots(1-x^{2m})\varphi_m(z)\\&=X'_0+\sum_{n=1}^{m}x^{n^2}(z^n+z^{-n})X'_n.\end{aligned}$$

当 $m\to\infty$ 时, $X'_n\to1$(对每个 $n\geqslant0$), 而上式左边即化为定理2中的左边, 由此即得雅可比恒等式. 证毕.

下面是雅可比恒等式一些有趣的应用.

定理2 我们有如下的恒等式

(1) $q_0q_2^2=\theta$, $q_0q_3^2=\sum\limits_{n=-\infty}^{\infty}(-1)^nx^{n^2}$, $q_0q_1^2=\sum\limits_{n=0}^{\infty}x^{n^2+n}$.

(2) $$\begin{aligned}q_0q_3&=\sum_{n=-\infty}^{\infty}(-1)^nx^{\frac12n(3n+1)}\\&=1+\sum_{n=1}^{\infty}(-1)^n\left(x^{\frac12n(3n-1)}+x^{\frac12n(3n+1)}\right).\end{aligned}$$

(3) $q_0q_1q_2\left(=\dfrac{q_0}{q_3}\right)=\sum\limits_{n=0}^{\infty}x^{\frac{1}{2}n(n+1)}$.

证明 (1) 在雅可比恒等式中取 $z=1$，便得到

$$q_0q_2^2=\prod_{n=1}^{\infty}(1-x^{2n})(1+x^{2n-1})(1+x^{2n-1})$$
$$=\sum_{n=-\infty}^{\infty}x^{n^2}=\theta(x).$$

若取 $z=-1$，便得到

$$q_0q_3^2=\prod_{n=1}^{\infty}(1-x^{2n})(1-x^{2n-1})^2=\sum_{n=-\infty}^{\infty}(-1)^nx^{n^2}.$$

若取 $z=x$，则得到第三个恒等式，详细证明留给读者.

(2) 在雅可比恒等式中取 $x=-y^{3/2}$, $z=y^{1/2}$，则

$$\prod_{n=1}^{\infty}(1-y^{3n})(1-y^{3n-1})(1-y^{3n-2})$$
$$=\sum_{n=-\infty}^{\infty}(-y^{3/2})^{n^2}y^{n/2}=\sum_{n=-\infty}^{\infty}(-1)^ny^{\frac{1}{2}n(3n+1)},$$

但是上式左边即为 $\prod\limits_{n=1}^{\infty}(1-y^n)=q_0q_3$，从而即得(2)式.

(3) 在雅可比恒等式中取 $x=y^{1/2}$, $z=y^{1/2}$ 即可. 详细证明留给读者.

上述所有恒等式(以及还有许多恒等式)都很有趣，但是对我们现在最有用的是第一个恒等式 $q_0q_2^2=\theta$. 因为由此可得到

$$(q_0q_2^2)^k=\theta^k=1+\sum_{n=1}^{\infty}r_k(n)x^n,$$

即对每个正整数 k, $r_k(n)$ 的母函数为 $q_0^kq_2^{2k}$. 从而椭圆模函数 q_0 和 q_2 与平方和表法个数建立了联系. 在以后两节里，我们直接由雅可比恒等式给出 $r_2(n)$ 的计算公式，然后由计算 $q_0^4q_1^8$ 的展开式系数得到 $r_4(n)$ 的计算公式.

3. $r_2(n)$计算公式

本小节我们直接由雅可比恒等式推出正整数n表示成两个整数平方和表法数$r_2(n)$的计算公式. 这是由 M. D. Hirschhorn 于1985年给出的证明(见 American Mathematical Monthly, 92(1985), 579—580), 为了避免用微积分, 我们又作了一些改动. 事实上, $r_2(n)$的这个公式是由高斯第一个证明的, 我们将在第 2.5 小节介绍高斯的证明.

定理3 设n为正整数. 以$d_1(n)$表示n的所有模4余1的正因子个数, 以$d_3(n)$表示n的所有模4余3的正因子个数, 即

$$d_1(n)=\sum_{\substack{d\mid n\\ d\equiv 1(\bmod 4)}}1,\ d_3(n)=\sum_{\substack{d\mid n\\ d\equiv 3(\bmod 4)}}1.$$

则 $r_2(n)=4(d_1(n)-d_3(n))$.

证明 在雅可比恒等式中, 令$z=-a^2y^{1/2}$, $x=y^{1/2}$, 则得到

$$\prod_{n=1}^{\infty}(1-y^n)(1-a^2y^n)(1-a^{-2}y^{n-1})$$
$$=\sum_{n=-\infty}^{\infty}(-1)^na^{2n}y^{\frac{1}{2}(n^2+n)}. \qquad ①$$

但是
$$\prod_{n=1}^{\infty}(1-a^{-2}y^{n-1})=(1-a^{-2})\prod_{n=1}^{\infty}(1-a^{-2}y^n),$$

从而将①式两边乘以a之后便得到

$$(a-a^{-1})\prod_{n=1}^{\infty}(1-a^2y^n)(1-a^{-2}y^n)(1-y^n)$$
$$=\sum_{n=-\infty}^{\infty}(-1)^na^{2n+1}y^{\frac{1}{2}(n^2+n)}.$$

将此式右边分别按偶数$n=2m$和奇数$n=2m-1$求和, 则它为

$$\sum_{m=-\infty}^{\infty} a^{4m+1}y^{2m^2+m}-\sum_{m=-\infty}^{\infty} a^{4m-1}y^{2m^2-m}.$$

在雅可比恒等式中取 $z=a^4y$, $x=y^2$,则得到

$$\prod_{n=1}^{\infty}(1+a^4y^{4n-1})(1+a^{-4}y^{4n-3})(1-y^{4n})$$
$$=\sum_{m=-\infty}^{\infty} a^{4m}y^{2m^2+m}.$$

若取 $z=a^4y^{-1}$, $x=y^2$,则得到

$$\prod_{n=1}^{\infty}(1+a^4y^{4n-3})(1+a^{-4}y^{4n-1})(1-y^{4n})$$
$$=\sum_{m=-\infty}^{\infty} a^{4m}y^{2m^2-m}.$$

综合以上各式,便得到

$$(a-a^{-1})\prod_{n=1}^{\infty}(1-a^2y^n)(1-a^{-2}y^n)(1-y^n)$$
$$=a\prod_{n=1}^{\infty}(1+a^4y^{4n-1})(1+a^{-4}y^{4n-3})(1-y^{4n})$$
$$-a^{-1}\prod_{n=1}^{\infty}(1+a^4y^{4n-3})(1+a^{-4}y^{4n-1})(1-y^{4n}),$$

于是

$$\prod_{n=1}^{\infty}\frac{(1-a^2y^n)(1-a^{-2}y^n)(1-y^n)}{1-y^{4n}}$$
$$=\frac{1}{a-a^{-1}}\Big[a\prod_{n=1}^{\infty}(1+a^4y^{4n-1})(1+a^{-4}y^{4n-3})$$
$$-a^{-1}\prod_{n=1}^{\infty}(1+a^4y^{4n-3})(1+a^{-4}y^{4n-1})\Big]$$
$$=\prod_{n=1}^{\infty}(1+a^4y^{4n-1})(1+a^{-4}y^{4n-3})$$
$$+\frac{a^{-1}}{a-a^{-1}}\Big[\prod_{n=1}^{\infty}(1+a^4y^{4n-1})(1+a^{-4}y^{4n-3})$$
$$-\prod_{n=1}^{\infty}(1+a^4y^{4n-3})(1+a^{-4}y^{4n-1})\Big]$$

$$=\prod_{n=1}^{\infty}(1+a^4y^{4n-1})(1+a^{-4}y^{4n-3})$$

$$\times\left[1+\frac{1}{a^2-1}\left(1-\prod_{n=1}^{\infty}\frac{(1+a^4y^{4n-3})(1+a^{-4}y^{4n-1})}{(1+a^4y^{4n-1})(1+a^4y^{4n-3})}\right)\right]$$

令 $a\to 1$，便得到

$$\prod_{n=1}^{\infty}\frac{(1-y^n)^3}{(1-y^{4n})(1+y^{4n-1})(1+y^{4n-3})}=1+M, \qquad ②$$

其中

$$M=\lim_{a\to 1}\frac{a^4-1}{a^2-1}\cdot\frac{1}{a^4-1}$$

$$\times\left[1-\prod_{n=1}^{\infty}\frac{(1+a^4y^{4n-3})(1+a^{-4}y^{4n-1})}{(1+a^4y^{4n-1})(1+a^{-4}y^{4n+3})}\right]$$

(令 $b=a^4$)

$$=2\lim_{b\to 1}\frac{1}{b-1}\left[1-\prod_{n=1}^{\infty}\frac{(1+by^{4n-3})(b+y^{4n-1})}{(1+by^{4n-1})(b+y^{4n-3})}\right]$$

(令 $b=1+c$)

$$=2\lim_{c\to 0}\frac{1}{c}\left[1-\prod_{n=1}^{\infty}\frac{(1+y^{4n-3}+cy^{4n-3})(1+y^{4n-1}+c)}{(1+y^{4n-1}+cy^{4n-1})(1+y^{4n-3}+c)}\right]$$

$$=2\cdot\lim_{c\to 0}\frac{1}{c}\left[1-\prod_{n=1}^{\infty}\frac{\left(1+\frac{y^{4n-3}}{1+y^{4n-3}}c\right)\left(1+\frac{1}{1+y^{4n-1}}c\right)}{\left(1+\frac{y^{4n-1}}{1+y^{4n-1}}c\right)\left(1+\frac{1}{1+y^{4n-3}}c\right)}\right]$$

$$=2\cdot\lim_{c\to 0}\frac{1}{c}\left[1-\prod_{n=1}^{\infty}\left(1+\frac{y^{4n-3}}{1+y^{4n-3}}c\right)\left(1+\frac{1}{1+y^{4n-1}}c\right)\right.$$

$$\left.\times\left(1-\frac{y^{4n-1}}{1+y^{4n-1}}c+\cdots\right)\left(1-\frac{c}{1+y^{4n-3}}+\cdots\right)\right]$$

$$=2\cdot\lim_{c\to 0}\frac{1}{c}\left[1-\prod_{n=1}^{\infty}\left(1+c\left(\frac{y^{4n-3}}{1+y^{4n-3}}+\frac{1}{1+y^{4n-1}}\right.\right.\right.$$

$$\left.\left.\left.-\frac{y^{4n-1}}{1+y^{4n-1}}-\frac{1}{1+y^{4n-3}}\right)+\cdots\right)\right]$$

$$=2\cdot\lim_{c\to 0}\frac{1}{c}\left[1-\prod_{n=1}^{\infty}\left(1+c\left(\frac{y^{4n-3}-1}{1+y^{4n-3}}-\frac{y^{4n-1}-1}{1+y^{4n-1}}\right)+\cdots\right)\right]$$

$$=2\cdot\lim_{c\to 0}\frac{1}{c}\cdot c\sum_{n=1}^{\infty}\left(\frac{y^{4n-1}-1}{1+y^{4n-1}}-\frac{y^{4n-3}-1}{1+y^{4n-3}}\right)$$

$$=2\cdot\sum_{n=1}^{\infty}\left(\frac{y^{4n-1}-1}{1+y^{4n-1}}-\frac{y^{4n-3}-1}{1+y^{4n-3}}\right)$$

$$=4\sum_{n=1}^{\infty}\left(\frac{y^{4n-1}}{1+y^{4n-1}}-\frac{y^{4n-3}}{1+y^{4n-3}}\right).$$

其中…均表示略去了 c 的二次方以上的诸项，这些项对极限值的贡献为 0. 于是代入 ② 式便得到

$$\prod_{n=1}^{\infty}(1-y^n)^3=\prod_{n=1}^{\infty}(1+y^{4n-3})(1+y^{4n-1})(1-y^{4n})$$

$$\times\left[1+4\sum_{n=1}^{\infty}\left(\frac{y^{4n-1}}{1+y^{4n-1}}-\frac{y^{4n-3}}{1+y^{4n-3}}\right)\right], \qquad ③$$

将 ③ 式除以

$$\prod_{n=1}^{\infty}(1+y^n)^2(1-y^n)=\prod_{n=1}^{\infty}(1+y^n)(1-y^{2n})$$

$$=\prod_{n=1}^{\infty}(1+y^{2n-1})(1+y^{2n})(1-y^{2n})$$

$$=\prod_{n=1}^{\infty}(1+y^{2n-1})(1-y^{4n})$$

$$=\prod_{n=1}^{\infty}(1+y^{4n-3})(1+y^{4n-1})(1-y^{4n}),$$

便得到

$$\prod_{n=1}^{\infty}\left(\frac{1-y^n}{1+y^n}\right)^2=1+4\sum_{n=1}^{\infty}\left(\frac{y^{4n-1}}{1+y^{4n-1}}-\frac{y^{4n-3}}{1+y^{4n-3}}\right). \qquad ④$$

但是 $\displaystyle\prod_{n=1}^{\infty}\left(\frac{1-y^n}{1+y^n}\right)=\prod_{n=1}^{\infty}\frac{(1-y^{2n-1})(1-y^{2n})}{(1+y^n)}$

$$=\prod_{n=1}^{\infty}(1-y^{2n-1})(1-y^n)$$

$$=\prod_{n=1}^{\infty}(1-y^{2n-1})(1-y^{2n-1})(1-y^{2n})$$

$$=\sum_{n=-\infty}^{\infty}(-1)^n y^{n^2}$$

（在雅可比恒等式中取 $z=-1$, $x=y$）

于是代入④式得到

$$\left(\sum_{n=-\infty}^{\infty}(-1)^n y^{n^2}\right)^2=1+4\sum_{n=1}^{\infty}\left(\frac{y^{4n-1}}{1+y^{4n-1}}-\frac{y^{4n-3}}{1+y^{4n-3}}\right).$$

令 $y=-x$，便有

$$\theta^2(x)=\left(\sum_{n=-\infty}^{\infty}x^{n^2}\right)^2$$

$$=1+4\sum_{n=1}^{\infty}\left(\frac{x^{4n-3}}{1-x^{4n-3}}-\frac{x^{4n-1}}{1-x^{4n-1}}\right). \quad ⑤$$

但是
$$\theta^2(x)=1+\sum_{m=1}^{\infty}r_2(m)x^m.$$

$$\sum_{n=1}^{\infty}\frac{x^{4n-3}}{1-x^{4n-3}}$$

$$=\sum_{n=1}^{\infty}x^{4n-3}(1+x^{4n-3}+x^{2(4n-3)}+x^{3(4n-3)}+\cdots)$$

$$=\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}x^{k(4n-3)}=\sum_{m=1}^{\infty}a_m x^m,$$

其中 a_m 等于不定方程 $zy=m$ 满足 $y\equiv-3\equiv1 \pmod 4$ 的正整数解 $(z, y)=(k, 4n-3)$ 的个数，即等于 m 的模 4 余 1 的正因子个数，即 $a_m=d_1(m)$．类似地，

$$\sum_{n=1}^{\infty}\frac{x^{4n-1}}{1-x^{4n-1}}=\sum_{m=1}^{\infty}d_3(m)x^m.$$

于是代入⑤式并比较等式两边 x^m 的系数，便得到

$$r_2(m)=4(d_1(m)-d_3(m)).$$

证毕．

【例】 $m=4500=2^2\cdot3^2\cdot5^3$．由于 m 的模 4 余 1 的正因子为 1, 5, 5^2, 5^3, 3^2, $3^2\cdot5$, $3^2\cdot5^2$ 和 $3^2\cdot5^3$，共 8 个，而模 4 余 3 的正因子为 3, $3\cdot5$, $3\cdot5^2$ 和 $3\cdot5^3$，共 4 个．因此

$$r_2(4500)=4(8-4)=16.$$

当 m 很大，特别是 m 有许多奇素因子时，上面的计算仍旧很麻烦．现在利用公式 $r_2(n)=4(d_1(n)-d_3(n))$ 来进一步研究函数 $r_2(n)$ 的性质，以简化计算 $r_2(n)$ 的工作量．

定义 定义在正整数集合上的函数 $f(n)$ 叫作数论函数．例如 $d_1(n)$，$d_3(n)$ 和 $r_2(n)$ 都是数论函数．

设 $f(n)$ 是数论函数．如果对任意两个互素的正整数 m 和 n，均有等式 $f(mn)=f(m)f(n)$，则称 f 是积性函数．

例如，取值恒为 0 或者恒为 1 的函数显然都是积性数论函数．初等数论中还有许多数论函数是积性的．我们这里只想证明

引理2 (i) 以 $d'(n)$ 表示正整数 n 的正因子个数，则 $d'(n)$ 是积性的．(ii) $\frac{1}{4}r_2(n)$ 是积性数论函数．

证明 (i) 设 n 和 m 是两个互素的正整数，如果 b 和 c 分别是 n 和 m 的正因子，即 $b|n$，$c|m$，则 $bc|nm$，从而 bc 是 nm 的正因子．反之，设 a 为 nm 的正因子，令

$$a=p_1^{\alpha_1}\cdots p_s^{\alpha_s}q_1^{\beta_1}\cdots q_t^{\beta_t}$$

是 a 的素因子分解式，其中 $p_1,\cdots,p_s,q_1,\cdots,q_t$ 为不同的素数．由于 $p_1|a$，$a|mn$，从而 p_1 必为 m 或 n 的因子．不妨设 $p_1|n$，由于 n 和 m 互素，从而 $p_1\nmid m$．于是由 $p_1^{\alpha_1}|mn$ 可知 $p_1^{\alpha_1}|n$．同样地，若 $p_2|n$，则必然 $p_2^{\alpha_2}|n$．再由 p_1 和 p_2 是不同的素数，可知 $p_1^{\alpha_1}p_2^{\alpha_2}|n$．所以，若 $p_1,\cdots,p_s$ 均除尽 n，而 $q_1,\cdots,q_t$ 均除尽 m，则 $b=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ 和 $c=q_1^{\beta_1}\cdots q_t^{\beta_t}$ 分别是 n 和 m 的正因子，而 $a=bc$．这就证明了，mn 的每个正因子均是 m 和 n 的两个正因子的乘积．现在设 b_1 和 b_2 均为 n 的正因子，c_1 和 c_2 均为 m 的正因子，并且 $b_1c_1=b_2c_2$，我们来证必然 $b_1=b_2$ 同时 $c_1=c_2$．事实上，由于 n 和 m 互素，从而它们的因子 b_1 和 c_2

互素．由 $b_1c_1=b_2c_2$ 知 $b_1|b_2c_2$．但是 b_1 与 c_2 互素，从而 $b_1|b_2$．完全类似地可知 $b_2|b_1$．但是 b_1 和 b_2 均是正整数，于是 $b_1=b_2$，从而 $c_1=c_2$．这就证明了：对于 n 和 m 的正因子 b 和 c 的不同取法，得到 nm 的不同的正因子．换句话说，如果 n 和 m 分别有 A 个和 B 个正因子 $\{n_1, \cdots, n_A\}$ 和 $\{m_1, \cdots, m_B\}$，则 $\{n_im_j|1\leqslant i\leqslant A,\ 1\leqslant j\leqslant B\}$ 恰好是 nm 彼此不同的全部正因子．于是 $d'(nm)=AB=d'(n)d'(m)$，即 $d'(n)$ 是积性的．

（ii）设 n 和 m 是互素的正整数．则由上面所证知 nm 的每个正因子 a 唯一可表成 $a=bc$，其中 b 和 c 分别是 n 和 m 的正因子．而 a 为奇数当且仅当 b 和 c 均为奇数．进一步，$a\equiv1 \pmod 4$ 当且仅当 $b\equiv c\equiv 1 \pmod 4$ 或者 $b\equiv c\equiv 3 \pmod 4$．于是 nm 的模 4 余 1 的正因子数 $d_1(nm)$ 等于 $d_1(n)d_1(m)+d_3(n)d_3(m)$．同样地，$nm$ 的模 4 余 3 的正因子数 $d_3(nm)$ 等于 $d_1(n)d_3(m)+d_3(n)d_1(m)$．于是

$$\begin{aligned}\frac{1}{4}r_2(nm)&=d_1(nm)-d_3(nm)\\&=(d_1(n)d_1(m)+d_3(n)d_3(m))\\&\quad-(d_1(n)d_3(m)+d_3(n)d_1(m))\\&=(d_1(n)-d_3(n))(d_1(m)-d_3(m))\\&=\frac{1}{4}r_2(n)\cdot\frac{1}{4}r_2(m).\end{aligned}$$

即 $\frac{1}{4}r_2(n)$ 是积性的．证毕．

一个积性数论函数 $f(n)$ 有什么优点呢？首先，如果 $f(n)$ 不恒为零，那么必然 $f(1)=1$．因为若对正整数 m，$f(m)\neq 0$，则 1 和 m 互素．于是 $f(m)=f(1\cdot m)=f(1)f(m)$．由 $f(m)\neq0$ 即知 $f(1)=1$．特别的，$\frac{1}{4}r_2(1)=1$，即 $r_2(1)=4$

(事实上，$x^2+y^2=1$ 有四个整数解 $(x, y)=(\pm 1, 0)$ 和 $(0, \pm 1)$)．其次，设 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$，其中 $p_1, \cdots, p_s$ 是不同的素数，则 $p_1^{\alpha_1}$ 与 $p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ 互素，因此

$$\begin{aligned} f(n) &= f(p_1^{\alpha_1})\cdot f(p_2^{\alpha_2}\cdots p_s^{\alpha_s}) \\ &= f(p_1^{\alpha_1})f(p_2^{\alpha_2})f(p_3^{\alpha_3}\cdots p_s^{\alpha_s}) \\ &= \cdots = f(p_1^{\alpha_1})f(p_2^{\alpha_2})\cdots f(p_s^{\alpha_s}). \end{aligned}$$

所以，为了求出 $f(n)$ 的表达式，只需对每个素数幂 p^α，计算 $f(p^\alpha)$ 就可以了．

例如对积性数论函数 $\frac{1}{4}r_2(n)$．我们现在计算 $\frac{1}{4}r_2(p^\alpha)$ 的值．当 $p=2$ 时，2^α 只有唯一的奇正因子 1．于是

$$\frac{1}{4}r_2(2^\alpha)=d_1(2^\alpha)-d_3(2^\alpha)=1-0=1.$$

(换句话说，对每个 $\alpha\geqslant 0$，不定方程 $x^2+y^2=2^\alpha$ 均只有 4 个整数解)若 $p\equiv 1 \pmod 4$，则 p^α 的所有正因子 $1, p, p^2, \cdots, p^\alpha$ 都是模 4 余 1 的因子．于是 $\frac{1}{4}r_2(p^\alpha)=\alpha+1$．最后若 $p\equiv 3 \pmod 4$，则 $1, p^2, p^4, \cdots$ 是模 4 余 1 的，而 $p, p^3, p^5, \cdots$ 是模 4 余 3 的．即

$$\frac{1}{4}r_2(p^\alpha)=\sum_{i=0}^{\alpha}(-1)^i=\begin{cases}0, & 若\ \alpha\ 为奇数;\\ 1, & 若\ \alpha\ 为偶数.\end{cases}$$

利用公式

$$\frac{1}{4}r_2(p_1^{\alpha_1}\cdots p_s^{\alpha_s})=\frac{1}{4}r_2(p_1^{\alpha_1})\times\frac{1}{4}r_2(p_2^{\alpha_2})\cdots\frac{1}{4}r_2(p_s^{\alpha_s}),$$

便给出 $r_2(n)$ 的下述公式．

定理 4 设正整数 $n=2^{\alpha_0}p_1^{\alpha_1}\cdots p_s^{\alpha_s}q_1^{\beta_1}\cdots q_t^{\beta_t}$，其中 $p_1, \cdots, p_s, q_1, \cdots, q_t$ 是不同的素数，并且

$$p_1 \equiv p_2 \equiv \cdots \equiv p_s \equiv 1 \pmod 4),$$
$$q_1 \equiv q_2 \equiv \cdots \equiv q_t \equiv 3 \pmod 4).$$
则当 $\beta_1, \cdots, \beta_t$ 至少有一个为奇数时，$r_2(n)=0$. 而当 $\beta_1, \cdots, \beta_t$ 均是偶数时，$r_2(n)=4(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1)$.

证明 由于

$$\frac{1}{4}r_2(n)=\frac{1}{4}r_2(2^{\alpha_0})\cdot\frac{1}{4}r_2(p_1^{\alpha_1})\cdot\cdots\cdot\frac{1}{4}r_2(p_s^{\alpha_s})$$
$$\cdot\frac{1}{4}r_2(q_1^{\beta_1})\cdot\cdots\cdot\frac{1}{4}r_2(q_t^{\beta_t}).$$

而 $\frac{1}{4}r_2(2^{\alpha_0})=1$. 如果 β_i 为奇数，则 $\frac{1}{4}r_2(q_i^{\beta_i})=0$，从而 $\frac{1}{4}r_2(n)=0$，即 $r_2(n)=0$. 如果 $\beta_1, \cdots, \beta_t$ 均为偶数，则

$$\frac{1}{4}r_2(q_i^{\beta_i})=1 \quad (1\leqslant i\leqslant t).$$

于是 $\frac{1}{4}r_2(n)=\frac{1}{4}r_2(p_1^{\alpha_1})\cdots\frac{1}{4}r_2(p_s^{\alpha_s})=(\alpha_1+1)\cdots(\alpha_s+1)$，

即 $r_2(n)=4(\alpha_1+1)\cdots(\alpha_s+1)$. 证毕.

用定理 4 来计算 $r_2(n)$ 就很方便了. 仍举前面的例子：$n=4500=2^2\cdot3^2\cdot5^3$. 由定理立刻得出

$$r_2(4500)=4\cdot(3+1)=16.$$

练习 试由定理 4 证明关于二平方和的高斯定理：正整数 n 为二平方和的充分必要条件是 n 的无平方因子部分 m' 没有模 4 余 3 的素因子.

4. $r_4(n)$ 计算公式

我们在前一小节计算出

$$q_0^2q_2^4=\theta^2=1+\sum_{n=1}^{\infty}r_2(n)x^n$$

$$=1+4\sum_{n=1}^{\infty}(u_{4n-3}-u_{4n-1})$$

$$=1+4(u_1-u_3+u_5-u_7+\cdots),$$

其中
$$u_r=\frac{x^r}{1-x^r}.$$

于是

$$q_0^4q_2^8=\theta^4=1+\sum_{n=1}^{\infty}r_4(n)x^n$$

$$=\left[1+4\sum_{n=1}^{\infty}(u_{4n-3}-u_{4n-1})\right]^2$$

$$=1+8\sum_{n=1}^{\infty}(u_{4n-3}-u_{4n-1})$$

$$+16\left[\sum_{n=1}^{\infty}(u_{4n-3}-u_{4n-1})\right]^2. \qquad ⑥$$

本节我们要把此式计算到底，并由此证明

定理5 对每个正整数 n，$r_4(n)$ 等于 n 的模 4 不同余 0 的所有正因子之和的 8 倍，即

$$r_4(n)=8\cdot\sum_{\substack{d\mid n\\ d\not\equiv 0(\mathrm{mod}\ 4)}}d.$$

这个定理的证明虽是一些初等计算但是复杂的．关键是把 ⑥ 式右边最后一项算出来．我们将计算分成几个引理．

引理3 $\sum_{m=1}^{\infty}u_m(1+u_m)=\sum_{n=1}^{\infty}nu_n.$

证明 易知

$$\frac{x^r}{(1-x^r)^2}=\frac{x^r}{1-x^r}+\frac{x^{2r}}{(1-x^r)^2}=u_r+u_r^2=u_r(1+u_r). \qquad ⑦$$

于是
$$\sum_{m=1}^{\infty}u_m(1+u_m)=\sum_{m=1}^{\infty}\frac{x^m}{(1-x^m)^2}$$

$$=\sum_{m=1}^{\infty}x^m(1+2x^m+3x^{2m}+4x^{3m}+\cdots)$$

$$=\sum_{m=1}^{\infty}(x^m+2x^{2m}+3x^{3m}+\cdots+nx^{nm}+\cdots)$$

$$=\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}nx^{nm}=\sum_{n=1}^{\infty}n\sum_{m=1}^{\infty}x^{nm}$$

$$=\sum_{n=1}^{\infty}n\cdot\frac{x^n}{1-x^n}=\sum_{n=1}^{\infty}nu_n.$$

其中我们用到了公式:

$$\frac{1}{(1-y)^2}=\sum_{n=0}^{\infty}(n+1)y^n=1+2y+3y^2+4y^3+\cdots.$$

这个公式很容易证明:

$$\frac{1}{(1-y)^2}=(1+y+y^2+y^3+\cdots)(1+y+y^2+y^3+\cdots)$$

$$\begin{aligned}=&1+y+y^2+y^3+\cdots\\ &+y+y^2+y^3+\cdots\\ &+y^2+y^3+\cdots\\ &+y^3+\cdots\\ =&1+2y+3y^2+4y^3+\cdots.\end{aligned}$$

这就证明了引理3.

引理4 $\sum_{m=1}^{\infty}(-1)^{m-1}u_{2m}(1+u_{2m})=\sum_{n=1}^{\infty}(2n-1)u_{4n-2}.$

证明 由⑦式可知

$$左边=\sum_{m=1}^{\infty}(-1)^{m-1}\frac{x^{2m}}{(1-x^{2m})^2}$$

$$=\sum_{m=1}^{\infty}(-1)^{m-1}\sum_{r=1}^{\infty}rx^{2mr}$$

$$=\sum_{r=1}^{\infty}r\sum_{m=1}^{\infty}(-1)^{m-1}x^{2mr}=\sum_{r=1}^{\infty}\frac{rx^{2r}}{1+x^{2r}}$$

$$=\sum_{r=1}^{\infty}\left(\frac{rx^{2r}}{1-x^{2r}}-\frac{2rx^{4r}}{1-x^{4r}}\right)$$

$$=\sum_{\substack{r=1\\2\nmid r}}^{\infty}\left(\frac{rx^{2r}}{1-x^{2r}}\right)\quad(令\ r=2n-1)$$

$$=\sum_{n=1}^{\infty}\frac{(2n-1)x^{4n-2}}{1-x^{4n-2}}=\text{右边}.$$

引理 5 设实数 θ 不为 2π 的整倍数，则

$$\left(\frac{1}{4}\operatorname{ctg}\frac{\theta}{2}+u_1\sin\theta+u_2\sin2\theta+\cdots\right)^2$$
$$=\left(\frac{1}{4}\operatorname{ctg}\frac{\theta}{2}\right)^2+c_0+\sum_{k=1}^{\infty}c_k\cos k\theta, \qquad ⑧$$

其中 $$c_0=\frac{1}{2}\sum_{n=1}^{\infty}nu_n,\quad c_k=u_k\left(1+u_k-\frac{k}{2}\right).$$
($k\geqslant1$ 时)

证明 ⑧式左边等于

$$\left(\frac{1}{4}\operatorname{ctg}\frac{\theta}{2}\right)^2+\frac{1}{2}\sum_{n=1}^{\infty}u_n\operatorname{ctg}\frac{\theta}{2}\sin n\theta$$
$$+\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}u_mu_n\sin m\theta\sin n\theta.$$

但是请大家验证下面的三角恒等式：

$$\frac{1}{2}\operatorname{ctg}\frac{\theta}{2}\sin n\theta=\frac{1}{2}+\cos\theta+\cos2\theta+\cdots$$
$$+\cos(n-1)\theta+\frac{1}{2}\cos n\theta,$$
$$2\sin m\theta\sin n\theta=\cos(m-n)\theta-\cos(m+n)\theta.$$

于是⑧式左边等于

$$\left(\frac{1}{4}\operatorname{ctg}\frac{\theta}{2}\right)^2+\sum_{n=1}^{\infty}u_n\left(\frac{1}{2}+\cos\theta+\cos2\theta+\cdots\right.$$
$$\left.+\cos(n-1)\theta+\frac{1}{2}\cos n\theta\right)$$
$$+\frac{1}{2}\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}u_mu_n[\cos(m-n)\theta-\cos(m+n)\theta].$$

将它与⑧式右边相比较，便知

$$c_0=\frac{1}{2}\sum_{n=1}^{\infty}(u_n+u_n^2)=\frac{1}{2}\sum_{n=1}^{\infty}nu_n.\ (\text{引理 3})$$

而当 $k\geqslant 1$ 时，

$$c_k=\frac{1}{2}u_k+\sum_{l=1}^{\infty}u_{k+l}+\sum_{l=1}^{\infty}u_l u_{k+l}-\frac{1}{2}\sum_{l=1}^{k-1}u_l u_{k-l}.$$

请大家利用 u_n 的定义直接验证以下两个恒等式：

$$u_l u_{k-l}=u_k(1+u_l+u_{k-l}),$$

$$u_{k+l}+u_l u_{k+l}=u_k(u_l-u_{k+l}).$$

于是 $$c_k=u_k\left(\frac{1}{2}+\sum_{l=1}^{\infty}(u_l-u_{k+l})-\frac{1}{2}\sum_{l=1}^{k-1}(1+u_l+u_{k-l})\right)$$

$$=u_k\left[\frac{1}{2}+u_1+u_2+\cdots+u_k\right.$$

$$\left.-\frac{1}{2}(k-1)-(u_1+u_2+\cdots+u_{k-1})\right]$$

$$=u_k\left(1+u_k-\frac{k}{2}\right).$$

引理 6

$$\left(\frac{1}{4}+\sum_{n=0}^{\infty}u_{4n+1}-\sum_{n=0}^{\infty}u_{4n+3}\right)^2=\frac{1}{16}+\frac{1}{2}\sum_{\substack{m=1\\4\nmid m}}^{\infty}mu_m.$$

证明 在引理 5 中取 $\theta=\frac{\pi}{2}$，则得到

$$\text{引理 6 左边}=\frac{1}{16}+\frac{1}{2}\sum_{n=1}^{\infty}nu_n+\sum_{m=1}^{\infty}(-1)^m c_{2m}$$

$$=\frac{1}{16}+\frac{1}{2}\sum_{n=1}^{\infty}nu_n+\sum_{m=1}^{\infty}(-1)^m u_{2m}(1+u_{2m}-m)$$

$$=\frac{1}{16}+\frac{1}{2}\sum_{m=1}^{\infty}(2m-1)u_{2m-1}+\sum_{m=1}^{\infty}mu_{2m}$$

$$+\sum_{m=1}^{\infty}(-1)^m u_{2m}(1+u_{2m})-m\sum_{m=1}^{\infty}(-1)^m u_{2m}$$

$$=\frac{1}{16}+\frac{1}{2}\sum_{m=1}^{\infty}(2m-1)u_{2m-1}$$

$$+\sum_{m=1}^{\infty}(-1)^m u_{2m}(1+u_{2m})+2\sum_{m=1}^{\infty}(2m-1)u_{4m-2}$$

$$=\frac{1}{16}+\frac{1}{2}\sum_{m=1}^{\infty}(2m-1)u_{2m-1}$$

$$+\sum_{m=1}^{\infty}(2m-1)u_{4m-2} \quad (\text{引理 } 4)$$

$$=\frac{1}{16}+\frac{1}{2}\sum_{\substack{n=1\\4\nmid n}}^{\infty}nu_n.$$

现在很容易得到定理 5. 由 ⑥ 的上式知

$$1+\sum_{k=1}^{\infty} r_4(n)x^k=\left[1+4\sum_{n=1}^{\infty}(u_{4n-3}-u_{4n-1})\right]^2$$

$$=1+8\sum_{\substack{m=1\\4\nmid m}}^{\infty} mu_m \quad (\text{引理 } 6)$$

$$=1+8\sum_{\substack{m=1\\4\nmid m}}^{\infty} m\sum_{n=1}^{\infty} x^{nm} \quad (\text{令 } k=nm)$$

$$=1+8\sum_{k=1}^{\infty}x^k\sum_{\substack{m\mid k\\4\nmid m}} m.$$

因此 $r_4(k)=8\sum\limits_{\substack{d\mid k\\4\nmid d}}d$. 这就证明了定理 5.

练习 1. 利用定理 5 证明拉格朗日定理: 每个正整数均可表为四个整数的平方和.

2. 设 n 是奇正整数, $\alpha\geqslant 1$. 求证:

$$r_4(2^{\alpha}n)=24r_4(n).$$

定理 6 (1) 以 $d(n)$ 表示正整数 n 的所有正因子之和, 则 $d(n)$ 是积性函数.

(2) $\frac{1}{8}r_4(n)$ 是积性函数.

证明 (1) 设 n 和 m 是互素的正整数. 若 $\{a_1, \cdots, a_s\}$ 是 n 的全部正整数因子, $\{b_1, \cdots, b_t\}$ 是 m 的全部正整数因子. 我们在前节已经证过, 当 n 和 m 互素时, $\{a_ib_j \mid 1\leqslant i\leqslant s, 1\leqslant j\leqslant t\}$ 恰好是 nm 的全部正整数因子. 于是

$$d(nm)=\sum_{i=1}^{s}\sum_{j=1}^{t}a_ib_j=\left(\sum_{i=1}^{s}a_i\right)\left(\sum_{j=1}^{t}b_j\right)=d(n)d(m).$$

(2) 令 $D(n)=\sum_{\substack{d\mid n\\4\nmid d}}d$, 则 $\frac{1}{8}r_4(n)=D(n)$. 我们现在来证 $D(n)$是积性函数. 设 n 和 m 是互素的正整数. 如果 n 和 m 均是奇数, 则 nm 也是奇数, 它们的每个因子均是奇数, 从而每个因子均不被 4 除尽. 因此

$$D(nm)=d(nm)=d(n)d(m)=D(n)D(m).$$

否则, 不妨设 n 为偶数, 则 m 必为奇数. 设 $n=2^{\alpha}\cdot n'$, 其中 $\alpha\geqslant 1$ 而 n' 为奇数. 若 n' 的所有正因子为 $\{a_1, \cdots, a_s\}$, m 的所有正因子为 $\{b_1, \cdots, b_t\}$, 则 a_i, b_j 均是奇数. 而 n 的不被 4 除尽的正因子为 $\{a_1, \cdots, a_s, 2a_1, \cdots, 2a_s\}$. 于是

$$D(n)=a_1+\cdots+a_s+2a_1+\cdots+2a_s=3d(n').$$

同样地, nm 的不被 4 除尽的正因子为$\{a_ib_j$ 和 $2a_ib_j \mid 1\leqslant i\leqslant s, 1\leqslant j\leqslant t\}$. 于是

$$D(nm)=3\sum_{i=1}^{s}\sum_{j=1}^{t}a_ib_j=3d(n')d(m),$$

而 $D(m)=d(m)$, 于是 $D(nm)=D(n)D(m)$. 证毕.

由于 $\frac{1}{8}r_4(n)$为积性函数, 于是像前小节对 $\frac{1}{4}r_2(n)$的讨论一样, 只需对 n 为素数幂的情形计算清楚即可. 设 $n=2^{\alpha}(\alpha\geqslant 1)$. 由于 n 只有正因子 1 和 2 是不被 4 除尽的. 于是 $\frac{1}{8}r_4(2^{\alpha})=1+2=3$, 即 $r_4(2^{\alpha})=3$. (注意对非零积性函数 $f(n)$, $f(1)=1$. 从而 $\frac{1}{8}r_4(1)=1$, 即 $r_4(1)=8$.)设 p 是奇素数, 则

$$\frac{1}{8}r_4(p^{\alpha})=D(p^{\alpha})=d(p^{\alpha})=1+p+p^2+\cdots+p^{\alpha}$$

$$=\frac{p^{\alpha+1}-1}{p-1}.$$

综合上述，我们便得到下面关于 $r_4(n)$ 的计算公式.

定理 7 设 n 为正整数，$n=2^{\alpha_0}p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，其中 $p_1, \cdots, p_s$ 是不同的奇素数. 则

(1) 当 n 为奇数时（即 $\alpha_0=0$ 时），

$$n=8\left(\frac{p_1^{\alpha_1}-1}{p_1-1}\right)\left(\frac{p_2^{\alpha_2}-1}{p_2-1}\right)\cdots\left(\frac{p_s^{\alpha_s}-1}{p_s-1}\right).$$

(2) 当 n 为偶数时（即 $\alpha_0\geqslant1$ 时），

$$n=24\left(\frac{p_1^{\alpha_1}-1}{p_1-1}\right)\left(\frac{p_2^{\alpha_2}-1}{p_2-1}\right)\cdots\left(\frac{p_s^{\alpha_s}-1}{p_s-1}\right).$$

证明 由于 $\frac{1}{8}r_4(n)$ 为积性函数，从而

$$\frac{1}{8}r_4(n)=D(n)=D(2^{\alpha_0})D(p_1^{\alpha_1})\cdots D(p_s^{\alpha_s}).$$

再利用上面给出的 $D(p^\alpha)$ 计算公式即可证明.

【例】 $n=1990=2\cdot5\cdot199$，而 199 为素数，则

$$r_4(n)=24\cdot(1+5)(1+199)=28800.$$

即将 1990 表成四整数平方和一共有 28800 种方法!

我们给出了 $r_2(n)$ 和 $r_4(n)$ 十分令人满意的计算公式. 我们在上节也叙述了 $r_3(n)$ 的公式，但是没有给出证明. 现在我们再简要地谈谈对于其他 k 值，如何计算 $r_k(n)$ 的公式？原则上来说，我们可以采用本节计算 $r_4(n)$ 的初等方法给出 $r_8(n)$ 和 $r_6(n)$ 的公式. 不过计算更为复杂. 并且因为是初等，所以需要很高的技巧. 就象加工一个零件，若用自动机床，只要按一下按钮，便可自动按步就班地进行. 但是若手工操作，则需要技艺高超的师傅. 计算 $r_k(n)$ 公式的“自动机床”已经在数学上被发明出来，这就是我们曾经提过的模形式理论. 公式

$r_6(n)$和 $r_8(n)$由雅可比于 1828 年用他的椭圆模函数求出. 爱森斯坦和闵柯夫斯基给出$r_5(n)$ 和 $r_7(n)$ 的公式; 柳维尔(Liouville) 于 1864 和 1866 年分别给出 $r_{10}(n)$ 和 $r_{12}(n)$的公式; Glaisher 于 1907 年给出 $r_{14}(n)$, $r_{16}(n)$和 $r_{18}(n)$的公式; 印度年轻早逝的天才数学家 Ramanujan于 1916 年给出 $r_{20}(n)$, $r_{22}(n)$ 和 $r_{24}(n)$ 的公式; 苏联数学家罗玛兹于 1949 年给出对 $k=9$, 11, 13, 15, 17, 19, 21 和 23 的 $r_k(n)$ 公式. 这些公式均是采用模形式理论构造出来的, 公式本身已相当复杂. 一般来说 k 为偶数时比 k 为奇数时求 $r_k(n)$的公式要容易, 这用模形式理论语言来说, 则是半整权模形式理论比整权模形式理论困难. 但这些事情只有在学到高级数论之后才能清楚, 我们就不多说了.

练习 利用上面 $r_8(n)$的公式, 证明:

(1) $\frac{1}{16}r_8(n)$是积性函数.

(2) 当 $\alpha\geqslant 1$ 时, $r_8(2^\alpha)=\frac{16}{7}(8^{\alpha+1}-15)$;

当 p 为奇素数时, $r_8(p^\alpha)=\frac{16(p^{3(\alpha+1)}-1)}{p^3-1}$

(3) $r_8(100)=16\times 71\times 15751$.

5. 再证 $r_2(n)$ 公式——兼谈高斯整数环

前面我们采用母函数方法, 并借助于雅可比恒等式和一系列计算, 得到 $r_2(n)$和 $r_4(n)$的具体公式. 在这一节我们换一换口味, 介绍高斯如何采用代数方法得到 $r_2(n)$的公式.

1801 年, 高斯研究二平方和问题, 即不定方程 $x^2+y^2=n$ 的整解问题. 他把这个方程写成如下形式:

$$n=(x+iy)(x-iy).$$

然后利用复数的性质，给出 n 何时为二平方和的判别方法. 由于 x 和 y 均是整数，所以问题只涉及这样的复数: $x+iy$，其中 x 和 y 均是整数. 由于高斯第一个深刻研究了这种复数的性质，后人把这种复数叫作*高斯整数*. 不难看出高斯整数之间作加、减和乘法运算，仍得到高斯整数. 具有这样性质的集合叫作是*环*(或者更确切地应说成是*交换环*，因为乘法满足交换律). 即我们把集合

$$\mathbf{Z}[i]=\{x+iy \mid x, y\in \mathbf{Z}\}$$

叫作*高斯整数环*，其中 $\mathbf{Z}$ 表示通常的整数环（全体整数也可作加、减、乘法，从而也是环）. 高斯深刻地研究了环 $\mathbf{Z}[i]$ 的数论性质，并由此算出 $r_2(n)$ 公式. 然而，高斯对 $\mathbf{Z}[i]$ 所作研究对数学所起的作用远不止于此，这是我们以后要谈的. 现在我们先谈清楚环 $\mathbf{Z}[i]$ 的数论性质，并随时与我们已经熟悉的整数环 $\mathbf{Z}$ 进行对比.

首先，正像 $\mathbf{Z}$ 中通常不能作除法一样，$\mathbf{Z}[i]$ 中通常也不能作除法. 例如 $1+2i$ 和 $1-2i$ 均属于 $\mathbf{Z}[i]$，但是

$$\frac{1+2i}{1-2i}=\frac{(1+2i)^2}{(1-2i)(1+2i)}=\frac{-3+4i}{5}$$

$$=\frac{-3}{5}+\frac{4}{5}i$$

不属于 $\mathbf{Z}[i]$，因为 $\frac{-3}{5}$ 和 $\frac{4}{5}$ 均不是整数. 所以 $\mathbf{Z}[i]$ 不是域. 现在我们可以像 $\mathbf{Z}$ 中那样定义 $\mathbf{Z}[i]$ 中的整除概念.

定义 设 α 和 β 为高斯整数，$\beta\neq 0$. 如果 α/β 仍是高斯整数，则称 β *整除* α，或称 α *被* β *整除*，表示成 $\beta\mid\alpha$. 如果 $\alpha/\beta\notin\mathbf{Z}[i]$，称 β 不整除 α，表示成 $\beta\nmid\alpha$.

练习　设 $\alpha, \beta, \gamma, \delta$ 为高斯整数，$\alpha \neq 0, \delta \neq 0$.

(1) 若 $\alpha | \beta$，则 $\alpha | \beta\gamma$.

(2) 若 $\alpha | \beta, \alpha | \gamma$，则 $\alpha | \beta \pm \gamma$.

(3) 若 $\alpha | \beta, \delta | \gamma$，则 $\alpha\delta | \beta\gamma$.

定义　设 $\alpha \in \mathbf{Z}[i]$，$\alpha = x + yi$. 定义 α 的范为

$$N(\alpha) = |\alpha|^2 = x^2 + y^2.$$

引理7　设 $\alpha, \beta \in \mathbf{Z}[i]$. 则

(1) $N(\alpha)$ 为非负整数. 并且 $N(\alpha) = 0 \leftrightarrow \alpha = 0$.

(2) $N(\alpha\beta) = N(\alpha)N(\beta)$.

(3) 若 $\alpha \neq 0, \alpha | \beta$，则 $N(\alpha) | N(\beta)$.

证明　(1) 是显然的. (2) $N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta)$. (3) 若 $\alpha | \beta$，则 $\gamma = \beta/\alpha$ 为高斯整数. 于是 $N(\gamma) \in \mathbf{Z}$. 而 $N(\beta) = N(\alpha\gamma) = N(\alpha)N(\gamma)$，由于 $N(\gamma) \in \mathbf{Z}$，从而 $N(\alpha) | N(\beta)$.

定义　设 $\alpha \in \mathbf{Z}[i]$，$\alpha \neq 0$. 如果存在 $\gamma \in \mathbf{Z}[i]$，使得 $\alpha\gamma = 1$，(这也相当于说 $\alpha | 1$) 则称 α 为 $\mathbf{Z}[i]$ 中的乘法可逆元，简称**可逆元**，并且 γ 叫作 α 的**逆**.

引理8　(1) 高斯整数 α 是可逆元的充要条件是

$$N(\alpha) = 1.$$

(2) $\mathbf{Z}[i]$ 中只有四个可逆元：± 1 和 $\pm i$.

证明　(1) 设 α 为 $\mathbf{Z}[i]$ 中可逆元，则有 $\gamma \in \mathbf{Z}[i]$，使得 $\alpha\gamma = 1$. 于是 $N(\alpha)N(\gamma) = N(1) = 1$. 但是 $N(\alpha)$ 和 $N(\gamma)$ 均是通常 ($\mathbf{Z}$ 中) 的整数，并且是非负的. 于是必然 $N(\alpha) = 1$. 反之，若 $N(\alpha) = \alpha\bar{\alpha} = 1$，则因 $\bar{\alpha}$ 也是高斯整数，从而由定义即知 α 为可逆元.

(2) 令 $\alpha = x + iy$ $(x, y \in \mathbf{Z})$. 则：α 为可逆元 $\leftrightarrow 1 = N(\alpha) = x^2 + y^2$. 但是这个不定方程只有四个解：$(x, y) = (\pm 1, 0)$,

$(0,\ \pm1)$. 它们分别对应四个可逆元 $\alpha=\pm1,\ \pm i$. 证毕.

由于可逆元只有四个 $\{\pm1,\ \pm i\}$, 可直接验证: 可逆元的逆也是可逆元, 可逆元之乘积仍是可逆元.

定义 设 α 和 β 是两个非零高斯整数. 如果存在可逆元 γ, 使得 $\alpha=\beta\gamma$, 则称 α 和 β 等价, 并表示成 $\alpha\sim\beta$. 换句话说, α 和 β 等价, 是指 $\alpha=\beta,\ -\beta,\ i\beta$ 或者 $-i\beta$.

不难验证: (1) $\alpha\sim\alpha$. (2) 若 $\alpha\sim\beta$, 则 $\beta\sim\alpha$. (3) 若 $\alpha\sim\beta,\ \beta\sim\gamma$, 则 $\alpha\sim\gamma$. 于是所有高斯整数分成许多等价类. 每个等价类包括四个高斯整数 $\{\pm\alpha,\ \pm i\alpha\}$. 特别地, 四个可逆元形成一个等价类 $\{\pm1,\ \pm i\}$. 而不同等价类中的两个高斯整数是彼此不等价的.

练习 (1) 若 $\alpha|\beta,\ \alpha\sim\gamma,\ \beta\sim\delta$, 则 $\gamma|\beta,\ \alpha|\delta$.

(2) 求证 $\alpha\sim\beta\Leftrightarrow\alpha|\beta$ 并且 $\beta|\alpha$.

(3) 以 $\bar{\alpha}$ 表示 α 的共轭, 若 $\alpha\sim\beta$, 则 $\bar{\alpha}\sim\bar{\beta}$. 若 $\alpha|\beta$, 则 $\bar{\alpha}|\bar{\beta}$.

在整数环 $\mathbf{Z}$ 中, 可逆元只有两个: ±1. 从而整数 a 和 b 等价的充要条件是 $a=\pm b$. 如果我们只谈正整数, 那么正整数只能与自身等价. 所以在研究正整数时可以不必引入等价这个概念. 一个正整数 p 叫作是素数, 是指只有 1 和 p 是它的正因子. 我们想在环 $\mathbf{Z}[i]$ 中也引入"素数"概念. 由于 $\mathbf{Z}[i]$ 中有较多的可逆元, 我们需要把环 $\mathbf{Z}$ 中素数概念换一个说法, 整数 p(可正可负)叫作是素数, 是指 $p\neq0$, 并且 $p\neq\pm1$ (即不是可逆元), 此外还要求 p 的每个因子或者是 ±1(即为可逆元), 或者是 $\pm p$(即与 p 等价). 这样的素数定义可以照搬到环 $\mathbf{Z}[i]$ 中.

定义 设 π 为 $\mathbf{Z}[i]$ 中非零非可逆元, 我们称 π 为高斯素数, 是指 π 的每个因子或者为可逆元, 或者是与 π 等价的高斯整数.

今后"素数"均指 $\mathbf{Z}$ 中的通常素数，用英文字母 p, q 等表示. 而高斯素数则用希腊字母 π 等表示.

现在我们给出高斯素数的一些例子.

引理 9 (1) 设 π 为高斯整数，并且 $N(\pi)=p$ 为素数，则 π 必为高斯素数.

(2) 若 π 为高斯素数，则共轭元 $\bar{\pi}$ 也是高斯素数.

(3) $1+i$ 是高斯素数. 若 p 是奇素数，如果 $p\equiv 3 \pmod 4$，则 p 也是高斯素数. 如果 $p\equiv 1 \pmod 4$，则存在高斯素数 π，使得 $N(\pi)=p$，并且 π 和 $\bar{\pi}$ 是不等价的高斯素数.

证明 (1) 由 $N(\pi)=p$ 知 $\pi\neq 0$，并且 π 不为可逆元. 进而若 $\pi=\alpha\beta$，其中 α, $\beta\in\mathbf{Z}[i]$. 则 $N(\alpha)N(\beta)=N(\alpha\beta)=N(\pi)=p$. 由于 $N(\alpha)$ 和 $N(\beta)$ 均为正整数，从而必然一个为 1 而另一个为 p，即 α 和 β 中必然有一个为可逆元，而另一个则与 π 等价. 换句话说，π 的每个因子或为可逆元或者与 π 等价. 于是 π 为高斯素数.

(2) 请读者自证.

(3) 由于 $N(1+i)=2$，从而由(1)知 $1+i$ 为高斯素数. 设 p 为素数并且 $p\equiv 3 \pmod 4$. 如果 $p=\alpha\beta$，其中 α, $\beta\in\mathbf{Z}[i]$. 则 $N(\alpha)N(\beta)=N(p)=|p|^2=p^2$. 于是 $N(\alpha)=1$, p 或者 p^2. 如果 $N(\alpha)=p$，令 $\alpha=x+iy$, x, $y\in\mathbf{Z}$，则 $x^2+y^2=N(\alpha)=p$. 但是 p 不为二平方和，从而 $N(\alpha)\neq p$. 若 $N(\alpha)=1$，则 α 为可逆元，而 β 与 p 等价. 若 $N(\alpha)=p^2$，则 $N(\beta)=1$，即 β 为可逆元而 α 与 p 等价. 这就表明 p 是高斯素数. 设 $p\equiv 1 \pmod 4$. 由二平方和定理知存在整数 x, y 使 $x^2+y^2=p$，于是 $N(x+iy)=p$. 由(1)知 $\pi=x+iy$ 是高斯素数. 最后证 $\pi=x+iy$ 与 $\bar{\pi}=x-iy$ 不等价，即 $x-iy$ 不能等于 $\pm(x+iy)$ 或 $\pm i(x+iy)$ 当中的任一个. 由 $xy\neq 0$ 和 $x\neq\pm y$ 很容易

验证这件事情.

事实上，用引理 9 (3) 中的办法可以给出全部高斯素数. 为了证明这件事，我们还需要研究高斯素数的性质. 读者不难发现，下面的概念、引理以及引理的证明都与整数环 $\mathbf{Z}$ 中的情形极为相似.

定义 非零高斯整数 α 和 β 叫作互素的，是指只有可逆元是它们的公因子.

引理 10 (1)（除法算式） 设 $\alpha, \beta\in\mathbf{Z}[i]$, $\beta\neq 0$. 则存在两个高斯整数 γ 和 δ, 使得 $\alpha=\gamma\beta+\delta$, 并且 $0\leqslant N(\delta)<N(\beta)$（请读者将 γ 和 δ 看成用 β 去除 α 的商和余数）.

(2) 若非零高斯整数 α 和 β 互素，则存在 $\gamma, \delta\in\mathbf{Z}[i]$, 使得 $\alpha\gamma+\beta\delta=1$.

(3) 设 π 是高斯素数, $\alpha, \beta\in\mathbf{Z}[i]$. 若 $\pi|\alpha\beta$, 则 $\pi|\alpha$ 或者 $\pi|\beta$.

证明 (1) α/β 是域 $\mathbf{Z}(i)$ 中元素，即 $\alpha/\beta=A+Bi$, 其中 A 和 B 是有理数. 我们总可找到整数 a, b, 使得 $|A-a|\leqslant 1/2$, $|B-b|\leqslant 1/2$. 令 $\gamma=a+bi$, 则 $\gamma\in\mathbf{Z}[i]$, 从而 $\delta=\alpha-\beta\gamma$ 也属于 $\mathbf{Z}[i]$. 并且

$$\begin{aligned}\delta&=(A+Bi)\beta-(a+bi)\beta\\&=[(A-a)+(B-b)i]\beta.\end{aligned}$$

于是
$$\begin{aligned}N(\delta)&=N(\beta)\cdot[(A-a)^2+(B-b)^2]\\&\leqslant N(\beta)\left[\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2\right]<N(\beta).\end{aligned}$$

(2) 设 α 和 β 是互素的高斯整数. 考虑集合

$$M=\{\alpha\gamma+\beta\delta\,|\,\gamma, \delta\in\mathbf{Z}[i]\}.$$

则集合 M 有以下两个性质:

(1) 若 $\mu, \nu\in M$, 则 $\mu\pm\nu\in M$. (因若 $\mu, \nu\in M$, 则

$\mu=\alpha\gamma_1+\beta\delta_1$, $\nu=\alpha\gamma_2+\beta\delta_2$, 其中 $\gamma_1, \delta_1, \gamma_2, \delta_2\in\mathbf{Z}[i]$. 于是 $\mu\pm\nu=\alpha(\gamma_1\pm\gamma_2)+\beta(\delta_1\pm\delta_2)$, 其中 $\gamma_1\pm\gamma_2$, $\delta_1\pm\delta_2\in\mathbf{Z}[i]$. 于是 $\mu\pm\nu\in M$).

(ii) 若 $\mu\in M$,则对每个 $\nu\in\mathbf{Z}[i]$, $\mu, \nu\in M$(请读者自证).

现在设 ε 是集合 M 中范最小的非零元素. (由于 $\alpha=\alpha\cdot1+\beta\cdot0$, $\beta=\alpha\cdot0+\beta\cdot1$ 均是 M 中非零元素,从而范最小的非零元素 ε 是存在的). 我们现在证明 ε 是 M 中每个高斯整数的因子: 设 $\mu\in M$, 由除法算式有 $\mu=\lambda\varepsilon+\nu$, 其中 $\lambda, \nu\in\mathbf{Z}[i]$并且 $0\leqslant N(\nu)<N(\varepsilon)$. 由于 $\mu\in M$, $\varepsilon\in M$, $\lambda\in\mathbf{Z}[i]$, 根据上述 M 的性质(i)和(ii)可知 $\nu=\mu-\lambda\varepsilon\in M$. 但是 $0\leqslant N(\nu)<N(\varepsilon)$,而 ε 是 M 中范最小的非零元素,从而必然 $\nu=0$, 即 $\mu=\lambda\varepsilon$. 这就表明 ε 是 M 中每个元素的因子. 特别因为 $\alpha, \beta\in M$, 从而 ε 是 α 和 β 的公因子. 但是 α 和 β 互素, 所以 ε 必为可逆元. 但是 $\varepsilon\in M$, 由 M 的定义即知存在 λ, $\mu\in\mathbf{Z}[i]$ 使得 $\varepsilon=\alpha\lambda+\beta\mu$. 从而 $1=\varepsilon\cdot\varepsilon^{-1}=\alpha\lambda\varepsilon^{-1}+\beta\mu\varepsilon^{-1}$. 取 $\gamma=\lambda\varepsilon^{-1}$, $\delta=\mu\varepsilon^{-1}$ 即可.

(3) 设 $\pi|\alpha\beta$. 如果 $\pi\nmid\alpha$, 则 π 和 α 必然互素(因为 π 和 α 的公因子 ε 也是 π 的因子, 从而 ε 必为可逆元或者 $\varepsilon\sim\pi$. 但是当 $\varepsilon\sim\pi$ 时 $\pi|\alpha$, 从而 ε 必为可逆元). 于是有 $\lambda, \mu\in\mathbf{Z}[i]$, 使得 $\alpha\lambda+\pi\mu=1$. 于是

$$\pi\,|\,(\alpha\beta)\lambda+\pi(\mu\beta)=\beta(\alpha\lambda+\pi\mu)=\beta.$$

证毕.

现在我们可以证明:

引理 11 每个高斯素数均与引理 9 的(3) 给出的某个高斯素数等价(从而引理 9 的(3)本质上给出全部高斯素数).

证明 设 π' 是任一高斯素数. 则 $N(\pi')=\pi'\overline{\pi'}=n$ 是大

于1的正整数，于是可写成一些素数之积：$n=p_1\cdots p_s$. 于是 $\pi'|n=p_1\cdots p_s$. 但是每个 p_i 均可分解成引理9的(3)中所述那些高斯素数或它们的等价高斯素数(因若 $p_i=2$, 则 $2=(1+i)(1-i)$ 而 $1-i$ 与 $1+i$ 等价；若 $p_i\equiv1\pmod 4$, 则 $p_i=\pi\bar{\pi}$, 其中 π, $\bar{\pi}$ 如引理9的(3)中所示；若 $p_i\equiv3\pmod 4$, 则 p_i 本身为高斯素数). 于是 $n=p_1\cdots p_s$ 可进一步写成 $n=\pi_1\pi_2\cdots\pi_r$, 其中 $\pi_j(1\leqslant j\leqslant r)$ 均是引理9的(3)中所述的高斯素数(或它们的等价元). 于是 $\pi'|\pi_1\pi_2\cdots\pi_r$. 再由引理10的(3)可知存在某个 $\pi_j(1\leqslant j\leqslant r)$, 使得 $\pi'|\pi_j$. 由于 π_j 是高斯素数，它的因子 π' 必或为可逆元、或者与 π_j 等价，由于 π' 也是高斯素数，从而 π' 不是可逆元，因此 π' 与 π_j 等价. 这就证明了引理11.

练习　写出范不超过20的所有高斯素数.

引理10的三条性质是高斯整数环 $\mathbf{Z}[i]$ 非常基本的性质. 在整数环 $\mathbf{Z}$ 中，我们可以用它们证明正整数唯一分解成素数之积. 现在我们也可以用它们来证明 $\mathbf{Z}[i]$ 也有类似的素因子唯一分解特征. 不过由于有较多的可逆元，从而叙述上要稍作改动.

定理8　(高斯整数环 $\mathbf{Z}[i]$ 的唯一因子分解定理)

(1) (存在性) $\mathbf{Z}[i]$ 中每个非零非可逆元均可表成有限个高斯素数之积.

(2) (唯一性) 设 $\alpha=\pi_1\pi_2\cdots\pi_s=\pi_1'\pi_2'\cdots\pi_t'$ 是 α 的两个分解式，其中 $\pi_i(1\leqslant i\leqslant s)$ 和 $\pi_j'(1\leqslant j\leqslant t)$ 均为高斯素数，则 $s=t$, 并且适当改变诸 π_j' 的下标，可使 $\pi_i\sim\pi_i'\ (1\leqslant i\leqslant s)$.

证明　(1) 存在性：设 $\alpha\in\mathbf{Z}[i]$, $\alpha\neq0$, 并且 α 不是可逆元，则 $N(\alpha)\geqslant2$. 我们对 $N(\alpha)$ 归纳证明. 当 $N(\alpha)=2$ 时，由引理9知 α 本身是高斯素数. 现设存在性对范小于 n 的高

斯整数均正确，而令 $N(\alpha)=n>2$. 由引理 9 的(3)知每个素数 p 均可表成一些高斯素数之积，而 n 又是一些素数之积，从而 n 也是一些高斯素数之积. 即 $\alpha\bar{\alpha}=N(\alpha)=\pi_1\pi_2\cdots\pi_s$，其中 π_i 均是高斯素数. 于是 $\pi_1|\alpha\bar{\alpha}$. 从而 $\pi_1|\alpha$ 或者 $\pi_1|\bar{\alpha}$. 而当 $\pi_1|\bar{\alpha}$ 时 $\bar{\pi}_1|\alpha$，这就表明必有高斯素数 π(等于 π_1 或者 $\bar{\pi}_1$)是 α 的因子. 于是 $\alpha=\pi\beta$，$\beta\in\mathbf{Z}[i]$. 由于 $N(\pi)>1$，从而 $N(\beta)<N(\alpha)$. 如果 $N(\beta)=1$，则 $\alpha=\pi\beta$ 本身就是高斯素数. 如果 $N(\beta)>1$，由于 $N(\beta)<N(\alpha)=n$，用归纳假设可知 β 可表成高斯素数之积，于是 $\alpha=\pi\beta$ 也可如此.

(2) 唯一性：我们仍对 $N(\alpha)$ 归纳. 如果 $N(\alpha)=2$，则 α 为高斯素数，并且由引理 10 知道范为 2 的高斯素数只有 $1+i$ 和与 $1+i$ 等价的数. 因此若 $2=\pi_1\pi_2\cdots\pi_s$，则 $4=N(\pi_1)\cdots N(\pi_s)$，于是每个 $N(\pi_i)$ 的范都是 2，所以 $s=2$，即 $2=\pi_1\pi_2$，并且 $\pi_1\sim\pi_2\sim(1+i)$，即 2 的分解是唯一的. 现设唯一性对所有范小于 n 的高斯整数均成立，而令 $N(\alpha)=n>2$. 如果 $\alpha=\pi_1\pi_2\cdots\pi_s=\pi_1'\cdots\pi_t'$. 则 $\pi_1|\pi_1'\cdots\pi_t'$. 于是存在某个 j 使 $\pi_1|\pi_j'$. 必要时改变一下 π_j' 的下标，不妨设 $j=1$，即 $\pi_1|\pi_1'$. 由于 π_1 和 π_1' 均为高斯素数，可知 $\pi_1\sim\pi_1'$(为什么?)即 $\pi_1'=\varepsilon\pi_1$，其中 ε 为可逆元. 于是

$$\alpha/\pi_1=\pi_2\cdots\pi_s=(\varepsilon\pi_2')\pi_3'\cdots\pi_t',$$

其中 $\varepsilon\pi_2'\sim\pi_2'$，故 $\varepsilon\pi_2'$ 仍为高斯素数. 由于 $N(\alpha/\pi_1)<N(\alpha)$，由归纳假设便知 $s-1=t-1$，即 $s=t$，并且适当改变下标可使 $\pi_2\sim\varepsilon\pi_2'\sim\pi_2'$，$\pi_3\sim\pi_3'$，…，$\pi_s\sim\pi_s'$. 证毕.

【例】 将 $10+11i$ 分解成高斯素数之积.

解：由于

$$\begin{aligned}N(10+11i)&=221=13\cdot17\\&=(2+3i)(2-3i)(1+4i)(1-4i),\end{aligned}$$

右边 4 个均是高斯素数，从而它们当中必有一个为 $10+11i$ 的因子．由此易知 $10+11i=(2-3i)(-1+4i)$ 为素因子分解式．

练习　将 $-19+7i$ 和 $12+9i$ 分解成高斯素数之积．

我们完成了代数准备工作，达到了我们的主要目的，即证明了高斯整数环 $\mathbf{Z}[i]$ 有唯一因子分解性质．现在我们用它来研究二平方和问题．我们已经知道，高斯整数环 $\mathbf{Z}[i]$ 与二平方和问题的基本联系在于：正整数 n 为二整数平方和的充分必要条件为 n 是某个高斯整数的范．

我们先来证明高斯定理：n 为二平方和的充分必要条件是 n 的无平方因子部分 m' 没有模 4 余 3 的素因子．

证明　令 $n=m^2m'$．如果 m' 没有模 4 余 3 的素因子，则 m' 是一些不同素数之积，这些素数为 2 或模 4 余 1，而它们均是某高斯整数的范(引理 9)．于是 m' 也是高斯整数的范，从而 $n=m^2m'$ 也是高斯整数的范，即 n 为二平方和．

如果 m' 有素因子 $p\equiv3 \pmod 4$，那么 $m'=pa$，其中 a 是与 p 互素的整数．设 $m=p^l\cdot b$，其中 $l\geqslant0$，$(b, p)=1$，则 $n=m^2m'=p^{2l+1}ab^2$，其中 $(ab^2, p)=1$．由于 $p\equiv3 \pmod 4$，从而 p 不但是通常的素数，它也是高斯素数(引理 9)．如果将 ab^2 分解成一些高斯素数之积：$ab^2=\pi_1\cdots\pi_s$，于是 $n=p^{2l+1}\pi_1\cdots\pi_s$ 是 n 在 $\mathbf{Z}[i]$ 中的一个素因子分解式，并且由 $p\nmid ab^2$，可知每个 π_i 均不与 p 等价．另一方面，如果 n 为二平方和，则有高斯整数 α，使得 $N(\alpha)=\alpha\bar{\alpha}=n$．设 $\alpha=p^s\pi'_1\cdots\pi'_t$ 是 α 表成高斯整数之积，其中 $\pi'_i\,(1\leqslant i\leqslant t)$ 均不与 p 等价，则 $\bar{\alpha}=p^s\bar{\pi}'_1\cdots\bar{\pi}'_t$，其中 $\bar{\pi}'_i\,(1\leqslant i\leqslant t)$ 也均是不与 p 等价的高斯整数．于是我们又得到 n 的第二个素因子分解式：

$$n=p^{2s}\pi'_1\cdots\pi'_t\bar{\pi}'_1\cdots\bar{\pi}'_t.$$

但是在这两个表达式中，所含 p 的个数是不一致的 $(2l+1\neq 2s)$，这就与分解的唯一性矛盾. 从而 n 不是二平方和. 证毕.

最后我们来推导 $r_2(n)$ 公式. 设 n 为二平方和，则 n 为高斯整数 $\alpha=A+iB(A,\ B\in\mathbf{Z})$ 的范，它对应 n 的一种表成二平方和的方法 $n=A^2+B^2$，与 α 等价的四个数 $\pm\alpha$，$\pm i\alpha$ 对应方程 $n=x^2+y^2$ 的四个不同的解 $(A,\ B)$，$(-A,\ -B)$，$(-B,\ A)$ 和 $(B,\ -A)$，这是由于 $-\alpha=-A-iB$，$i\alpha=-B+iA$，$-i\alpha=B-iA$. 于是，范为 n 的高斯整数等价类数为 $\frac{1}{4}r_2(n)$. 以下简记 $D(n)=\frac{1}{4}r_2(n)$. 我们先证 $D(n)$ 是积性函数.

引理 12 (1) 设 n 和 m 是互素的正整数，

$$\alpha\in\mathbf{Z}[i],\ N(\alpha)=nm,$$

则存在 $\beta,\ \gamma\in\mathbf{Z}[i]$，使得 $\alpha=\beta\gamma$，并且 $N(\beta)=n$，$N(\gamma)=m$.

(2) 进而若又有 $\beta',\ \gamma'\in\mathbf{Z}[i]$，使得 $\alpha=\beta'\gamma'$，$N(\beta')=n$，$N(\gamma')=m$，则 $\beta\sim\beta'$，$\gamma\sim\gamma'$.

(3) $D(n)$ 为积性函数.

证明 (1) 设 $\alpha=\pi_1\cdots\pi_s\pi'_1\cdots\pi'_t$，则

$$N(\pi_1)\cdots N(\pi_s)N(\pi'_1)\cdots N(\pi'_t)=nm.$$

由于每个 $N(\pi_i)$ 或 $N(\pi'_j)$ 均是素数或素数平方，而 n 和 m 互素，从而每个 $N(\pi_i)$ 或 $N(\pi'_j)$ 恰好除尽 n 和 m 当中的一个. 不妨设 $N(\pi_i)\mid n,\ N(\pi'_j)\mid m\quad(1\leqslant i\leqslant s,\ 1\leqslant j\leqslant t)$

令
$$\beta=\pi_1\cdots\pi_s,\ \gamma=\pi'_1\cdots\pi'_t.$$

则
$$\alpha=\beta\gamma,\ N(\beta)N(\gamma)=nm.$$

由于 $N(\beta)$ 与 m 互素，从而 $N(\beta)\mid n$. 同样可知 $N(\gamma)\mid m$. 再由 $N(\beta)N(\gamma)=nm$ 便知 $N(\beta)=n$，$N(\gamma)=m$.

(2) 在假设条件下，$\alpha\beta=\alpha'\beta'$. 由于 $N(\alpha)=\alpha\bar{\alpha}=n$ 和

$N(\beta')=\beta'\bar{\beta}'=m$ 互素，可知 α 与 β' 互素．于是 $\alpha|\alpha'$．类似可证 $\alpha'|\alpha$．于是 $\alpha\sim\alpha'$，从而 $\beta\sim\beta'$．

(3) 由(1)和(2)所证，可知当 β 和 γ 分别通过范为 n 和 m 的高斯整数等价类代表时，$\beta\gamma$ 恰好通过范为 nm 的高斯整数等价类全体代表．从而范为 nm 的高斯整数等价类数 $D(nm)$ 恰好等于 $D(n)D(m)$．

由于 $D(n)$ 为积性函数，我们只需考查 $D(p^\alpha)$ 的值即可．对于 $p=2$，只有一个范为 2 的高斯素数(等价类)，即 $1+i$．从而不计等价，范为 2^α 的高斯整数只有 $(1+i)^\alpha$．于是 $D(2^\alpha)=1$．若 $p\equiv1(\mathrm{mod}\,4)$，则范为 p 的高斯素数(等价类)只有两个：$\beta=a+bi$ 和 $\bar{\beta}$，其中 $a^2+b^2=p$．于是范为 p^α 的高斯整数共有(不计等价)：β^α，$\beta^{\alpha-1}\bar{\beta}$，$\beta^{\alpha-2}\bar{\beta}^2$，…，$\beta\bar{\beta}^{\alpha-1}$ 和 $\bar{\beta}^\alpha$，从而 $D(p^\alpha)=\alpha+1$．最后若 $p\equiv3(\mathrm{mod}\,4)$，则 p 本身为高斯素数．于是当 α 为偶数时，$D(p^\alpha)=1$，(因 $p^{\alpha/2}$ 是唯一的范为 p^α 的高斯整数)；而当 α 为奇数时，$D(p^\alpha)=0$．

这样一来，我们算出所有 $D(p^\alpha)$ 值均与第 3 小节一致．由于 $D(n)$ 为积性函数，从而便得到第 3 小节关于 $D(n)$ 的公式．于是我们用代数方法再一次得到 $r_2(n)=4D(n)$ 的计算公式．

幕 间 休 息
——漫谈代数数论

我们的节目已经进行了大半，经过那么多的推导和演算，读者可能感到疲乏(当然我们也希望大家得到一点乐趣)，现在是需要幕间休息，喜剧演员登场，作轻松表演的时候了．下面我们讲一些数论上的典故，还是从高斯说起．

为了研究二平方和问题，高斯深入地研究了环 $\mathbf{Z}[i]$．最重要的事情是他把整除性、素数等概念推广到 $\mathbf{Z}[i]$ 中，并且证明了素因子唯一分解定理．然后用这些研究成果彻底解决了二平方和问题，并算出 $r_2(n)$ 的计算公式，我们在第 2.5 小节讲述了这件事．

事实上，高斯对任意正定二元二次型 $f(x, y)=ax^2+bxy+cy^2$，研究了不定方程 $f(x, y)=n$ 的整数解问题．不妨设 $(a, b, c)=1$．如果 $f(x, y)$ 的判别式为 $D=b^2-4ac$，则由于 f 是正定的，从而 $D<0$，并且 $D\equiv 1$ 或 $0 \pmod 4$．而不定方程 $f(x, y)=n$ 的整解问题归结于研究环

$$R_D=\mathbf{Z}\left[\frac{D+\sqrt{D}}{2}\right]=\left\{A+B\cdot\frac{D+\sqrt{D}}{2}\,\middle|\,A, B\in\mathbf{Z}\right\} \quad ①$$

的性质(请大家验证 R_D 是环，主要困难在于证明 R_D 中可作乘法)．例如对二平方和问题，$f=x^2+y^2$，$D=-4$，于是

$$R_{-4}=\{A+B(-2+i)\,|\,A, B\in\mathbf{Z}\}=\{C+Di\,|\,C, D\in\mathbf{Z}\}.$$

即 R_{-4} 为高斯整数环 $\mathbf{Z}[i]$．

练习 (1) 若 $D\equiv 0 \pmod 4$，令 $d=\frac{D}{4}$，则

$$R_D=\mathbf{Z}[\sqrt{d}]=\{A+B\sqrt{d}\mid A,B\in\mathbf{Z}\}.$$

(2) 若 $D\equiv 1 \pmod 4$，则

$$R_D=\mathbf{Z}\left[\frac{D+\sqrt{D}}{2}\right]=\left\{\frac{A+B\sqrt{D}}{2}\,\middle|\,A,\ B\in\mathbf{Z},\ \ A\equiv B \pmod 2\right\}.$$

如果 R_D 也具有素因子唯一分解性质，那么对于判别式为 D 的二元二次型 $f(x, y)$，我们可以完全一样地研究不定方程 $f(x, y)=n$ 的整数解问题．例如对于 $f(x, y)=x^2+2y^2$，$D=-8$．于是 $R_{-8}=\mathbf{Z}[\sqrt{-2}]=\{A+\sqrt{-2}B\mid A, B\in\mathbf{Z}\}$．可以证明 R_{-8} 具有素因子唯一分解性质．然后仿照 $f(x, y)=x^2+y^2$ 和 $R_{-4}=\mathbf{Z}[\sqrt{-1}]$的情形，就可研究方程 $x^2+2y^2=n$．我们把整个工程编成一个大练习放在本节末尾．

高斯作了大量计算工作，以验证环 R_D 是否有素因子唯一分解特性．他发现当 $D=-1, -2, -3, -7, -11, -19, -43, -67$ 和 -163 时，R_D 具有素因子唯一分解特性，而他所计算的其他 R_D 均没有这个特性（从解不定方程的观点看来，这是令人扫兴的）．于是在上世纪初，高斯凭着他的手算结果提出下列猜想：当 $D<0$ 时，只有上述九个环 R_D 具有素因子唯一分解特性．这个猜想在一百多年以后于 1972 年才由英国数学家贝克尔 (Baker) 和美国数学家斯塔克 (Stark) 相互独立地证明，其所用的工具是超越数论和模形式理论．（又是模形式理论！）另一方面，当 $D>0$，并且 $D\equiv 1$ 或 $0 \pmod 4$时，由 ① 式定义的 R_D 仍旧是环．用环 R_D 可以研究不定方程 $f(x, y)=n$ 的整数解，其中 $f(x, y)$ 是判别式为 $D(>0)$的非正定的二元二次型．对于这种环高斯也手算了大量的例子，发现有许多 $R_D(D>0)$具有素因子唯一分解特性．他大胆地猜想：存在无限多个正整数 D，使得 R_D 有素因

子唯一分解特性. 这个问题经过一百多年许多大数学家的研究, 至今仍未解决(既没有证明, 也没有推翻). 这是数论中遗留下来的著名猜想当中的一个.

高斯这种研究思想受到后来许多大数学家的重视, 用它来研究其他不定方程的整数解. 其中最著名的不定方程当然首推费尔马方程

$$x^n+y^n=z^n.$$

费尔马猜想当 $n\geqslant 4$ 时, 该方程没有整数解 (x, y, z) 使得 $xyz\neq 0$. 费尔马本人对 $n=4$ 证明了此猜想. 不难看出, 如果对每个奇素数 $n=p$, 均能证明此猜想成立, 那么这个猜想便彻底证明了. (为什么?)于是后人集中考虑 n 为奇素数的情形. 1770 年, 欧拉证明了 $n=3$ 的情形; 1825 年勒让得证明了 $n=5$ 的情形; 1832 年狄里赫利证明了 $n=7$ 的情形. 他们的证明采用了愈来愈复杂的计算. 1847—1849 年, 德国数学家库默尔(Kummer)迈出了重大的一步, 他系统地发展了高斯的思想, 即把费尔马方程 $x^p+y^p=z^p$ 放到比 $\mathbf{Z}$ 更大的环

$$\mathbf{Z}[\zeta_p]=\{a_0+a_1\zeta_p+a_2\zeta_p^2+\cdots+a_{p-2}\zeta_p^{p-2}\,|\,a_0, a_1, a_2, \cdots, a_{p-2}\in\mathbf{Z}\}$$

上去考虑, 其中 $\zeta_p=e^{\frac{2\pi i}{p}}$(请读者利用关系式 $1+\zeta_p+\zeta_p^2+\cdots+\zeta_p^{p-1}=(1-\zeta_p^p)/(1-\zeta_p)=0$ 来证明 $\mathbf{Z}[\zeta_p]$ 是环). 这是因为在环 $\mathbf{Z}[\zeta_p]$ 中, 即加入数 ζ_p 之后, 费尔马方程 $x^p+y^p=z^p$ 便可改写成

$$(x-z)(x-\zeta_p z)(x-\zeta_p^2 z)\cdots(x-\zeta_p^{p-1}z)=-y^p.$$

如果 x, y, z 均是整数, 那么 $x-z, x-\zeta_p z, \cdots, x-\zeta_p^{p-1}z$ 均属于环 $\mathbf{Z}[\zeta_p]$. 从而方程两边是 $\mathbf{Z}[\zeta_p]$ 中一些元素的乘积. 库默尔认为 $\mathbf{Z}[\zeta_p]$ 具有素因子唯一分解特性, 利用这个性质, 库

默尔兴奋地宣布：他证明了费尔马猜想！但不久他意识到 $\mathbf{Z}[\zeta_p]$ 具有素因子唯一分解性质这件事可能并不是对所有奇素数 p 均正确。于是他作了大量计算(这个计算比环 R_D 还要复杂得多)．发现当 $p=3, 5, 7, 11, 13, 17$ 和 19 时，$\mathbf{Z}[\zeta_p]$ 有素因子唯一分解特性(从而他用统一的方法证明了当 p 是不超过 19 的奇素数时，费尔马猜想均成立)．而 $\mathbf{Z}[\zeta_{23}]$ 没有这个特性．库默尔于是猜想：当 p 是大于 19 的素数时，$\mathbf{Z}[\zeta_p]$ 均没有素因子唯一分解特性，这个猜想直到 1976 年才被美国数学家证明，利用的是解析数论工具．

库默尔没有完全解决费尔马猜想，但他毫不甘心，竭力修补他的证明，终于得到更好的结果．例如根据他的结果，可知对于 100 以内的奇素数 p，除了 37 和 67 以外，费尔马猜想均成立．与过去相比，这无疑是一项光辉的成就．但是更重要的是，他的工作促进了代数学的发展．例如他对于素因子分解不唯一的环 $\mathbf{Z}[\zeta_p]$，考虑对所谓"理想数"进行分解，而这个理想数便是近世代数中所谓环的"理想"这一概念的前身．高斯和库默尔这种把纯粹是整数环 $\mathbf{Z}$ 上的初等数论问题放到各种更大的数环和数域上去研究，引进了许多新的代数概念和结果，并把这种代数方法应用到数论研究中，开创了数论一个新的分支——代数数论．

十九世纪后半叶一直到第二次世界大战前夕，是代数数论的黄金时代．代数数论的圣地是德国的哥庭根大学，希尔伯特是其中的领袖人物．1898 年，希尔伯特写了一本著名的《数论报告》，对于代数数论作了极为详细的研究．1900 年，希尔伯特站在通往新世纪的门坎上，应邀在第二次国际数学家大会上作了题为"数学问题"的报告．他一开始便鼓动人心地问道："我们当中有谁不愿意揭开遮住未来的面纱，看一看

在今后的世纪里我们这门科学发展的前景和奥秘呢？我们下一代的主要数学思潮将追求什么样的特殊目标？在广阔而丰富的数学思想领域，新世纪将会带来什么样的新方法和新结果……"随后，他提了二十三个著名的数学问题，其中有四个是属于代数数论的．九十年来，人们对这些问题的研究在世界数学发展中起了很大的作用．我们在本书第四章中将要介绍其中一个问题，即关于多项式平方和的希尔伯特第十七问题．

练习

1．证明 $\mathbf{Z}[\sqrt{-2}]=\{A+\sqrt{-2}\,B\,|\,A,\,B\in\mathbf{Z}\}$ 为环，并且乘法可逆元只有 ± 1．

2．定义 $\mathbf{Z}[\sqrt{-2}]$中元素等价、元素的范以及"素数"概念．

3．证明 $\mathbf{Z}[\sqrt{-2}]$有除法算式，从而有素因子唯一分解性质．

4．素数 p 为 $\mathbf{Z}[\sqrt{-2}]$中元素的范，当且仅当 $p=2$ 或者 $p\equiv 1,\ 3\pmod 8$．$\left(\text{提示：当 } p \text{ 为奇素数时，}\left(\frac{-2}{p}\right)=(-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}}.\right)$

5．决定 $\mathbf{Z}[\sqrt{-2}]$中全部"素数"．

6．设 n 为正整数，求证：不定方程 $x^2+2y^2=n$ 有整数解的充分必要条件是 n 的无平方因子部分没有模 8 余 5 或余 7 的素因子．

7．以 $R(n)$表示方程 $x^2+2y^2=n$ 的整数解个数，证明 $\frac{1}{2}R(n)$是积性函数．

8．设 $n=2^{\alpha_0}p_1^{\alpha_1}\cdots p_s^{\alpha_s}q_1^{\beta_1}\cdots q_t^{\beta_t}$，其中 $\alpha_0\geqslant 0$，$\alpha_1,\ \cdots,\ \alpha_s\geqslant 1$，$\beta_1,\ \cdots,\ \beta_t\geqslant 1$．$p_1,\ \cdots,\ p_s,\ q_1,\ \cdots,\ q_t$ 是不同的素数，并且 $p_i\equiv 1$ 或 $3\pmod 8$ $(1\leqslant i\leqslant s)$，$q_j\equiv 5$ 或 $7\pmod 8$ $(1\leqslant j\leqslant t)$．则当 $\beta_1,\ \cdots,\ \beta_t$ 当中至少有一个奇数时，$R(n)=0$．而当 $\beta_1,\ \cdots,\ \beta_t$ 均是偶数时，$R(n)=2(\alpha_1+1)\cdots(\alpha_s+1)$．

三、-1 是平方和吗？

-1 是平方和吗？即方程 $x_1^2+\cdots+x_n^2=-1$ 是否可解？这个问题显然与要求解在什么范围有关．例如在实数域 $\mathbf{R}$ 或者它的任何子域中，-1 显然不是平方和（域 F 包含在域 E 中，称 F 为 E 的子域．例如有理数域 $\mathbf{Q}$ 是 $\mathbf{R}$ 的子域）．而 -1 在复数域 $\mathbf{C}$ 中显然是平方和：$-1=i^2+0^2$．那么在一般情形下，对于任意给定的一个域 F，如何判别 -1 是否为 F 中元素的平方和？这个问题是很不简单的．

1926 年，德国著名数学家阿廷（E. Artin）和施莱尔（Schreier）对于 -1 在任意域中能否表成平方和问题建立了十分漂亮的理论．这个理论的大部分内容是初等的．1965—1970 年，德国另一位数学家费斯特（Pfister）对这问题又作出重要的贡献，他所研究的问题是：如果 -1 在域 F 中可表成平方和，即域 F 中存在元素 $a_1, \cdots, a_n$，使得 $-1=a_1^2+\cdots+a_n^2$，那么 n 的最小值是多少？例如在复数域中可取 $n=1$．更一般地，对每个包含 $i^2=-1$ 的域 F，n 均可取为 1．再如对域 $\mathbf{Q}(\sqrt{-2})=\{a+b\sqrt{-2}\mid a, b\in\mathbf{Q}\}$．由于 $i\notin\mathbf{Q}(\sqrt{-2})$，从而 n 不能取为 1，而由 $-1=(\sqrt{-2})^2+1^2$ 可知在 $\mathbf{Q}(\sqrt{-2})$ 中 n 的最小值为 2．费斯特的一个漂亮结果是：在每个域中，n 的最小值只能是 1, 2, 4, 8, … 这样一些 2 的方幂！特别地，若 -1 在某域 F 中是七平方和，则也必然是四平方和．费斯特的理论本质上也是初等的，运用了很奇特的技巧．

本章的主要内容是介绍阿廷-施莱尔理论和费斯特的理论，并且举一些有趣的例子. 对于大多数结果我们均给出初等证明，但有些地方涉及比较高深的知识，不是三言两语能够说清楚的，我们便只作些介绍.

1. -1就是一切

为什么对 -1 是否为平方和特别感兴趣？这是因为：对于任意域 F，如果 -1 是 F 中元素的平方和，那么 F 中每个元素均可表成 F 中元素的平方和. 这就是本小节标题的确切含义. 我们在这小节里要证明这个令人惊讶的事实（引理3的(2)）. 但是要说明一点，就是在我们今后讨论的所有域中，$2\neq 0$，从而 2 是域中可逆元，即 $\frac{1}{2}$ 在域中是有意义的. 大家也许会奇怪：在域中 2 怎么会等于 0？但事实上这样的域是存在的，甚至最最简单的域就是这样的域，即域中只有两个元素：0 和 1，其四则运算与通常一样，只是规定 $1+1=0$. 在这个二元域中 $2(=1+1)$ 便等于 0.

阿廷和施莱尔把在其中 -1 不是平方和的域叫作形式实域. 例如实数域（和它的任意子域）是形式实域，从而形式实域就是实数域的一种推广. 我们的目标是要判别 -1 是否为域 F 中平方和，即要给出 F 是否为形式实域的一种判别方法. 大家知道，通常实数域中任意两个不同的实数 α 和 β 可以比较大小（即次序）：$\alpha>\beta$，即指 $\alpha-\beta$ 是正数. 所有的实数可分成三类：正实数、负实数和 0. 并且正实数相加及相乘仍是正实数. 阿廷和施莱尔发现这样的性质是任意形式实域所固有的. 为此，我们首先引入如下定义：

定义 域 F 叫作有序的，是指 F 中存在子集合 P 具有下列性质：

(1) 域 F 分拆成$\{0\}$，P 和 $-P$ 的并，其中 $-P=\{-a|a\in P\}$. 换句话说，F 中每个元素恰好属于这三个子集当中的一个.

(2) 若 $x, y\in P$，则 $x+y$, $xy\in P$. 即 P 中可作加法和乘法.

P 中元素叫作正元素. $-P$ 中元素叫作负元素. 由此可定义域 F 中元素的大小(即次序)关系：对于任意两个元素 a 和 $b\in F$. 定义 $a>b$(或写成 $b<a$)是指 $a-b\in P$. 称作 a 比 b 大(或 b 比 a 小). 从而正元素集合 P 有时也叫作域 F 的一个序.

【例 1】 实数域 $\mathbf{R}$ 是有序域，其中 P 取为通常的正实数集合. 事实上，实数域 $\mathbf{R}$ 只有唯一的序(这由下面的引理 1 即知).

若 F 是有序域，P 是它的正元集合. 对于 F 的每个子域 E，令 $P'=E\cap P$，则 P' 满足定义中的两个条件(请读者自证)，从而给出 E 的一个序. 换句话说，E 中元素 a 是正元素(负元素)当且仅当 a 在 F 中是正元素(负元素). 这说明：有序域的每个子域均是有序域.

【例 2】 我们举例说明一个域中可以存在许多个不同的序，取 $F=\mathbf{R}(x)$，即实数域上的有理函数域. F 中每个元素可表示成

$$\alpha=\frac{f(x)}{g(x)},$$

其中 $f(x)$, $g(x)$ 均是实系数多项式，其中 $g(x)\neq 0$. 令

$$f(x)=a_m x^m+a_{m-1}x^{m-1}+\cdots+a_n x^n\neq 0,$$

$$g(x)=b_s x^s+b_{s-1}x^{s-1}+\cdots+b_t x^t\neq 0,$$

其中 a_m, a_n, b_s, b_t 均不为零. 我们定义

$$P_1=\left\{\alpha=\frac{f(x)}{g(x)}\neq 0 \;\middle|\; a_m b_s\text{为正实数}\right\}.$$

请读者证明 P_1 满足定义中两个条件, 从而 P_1 给出域 F 的一个序. 如果我们定义

$$P_2=\left\{\alpha=\frac{f(x)}{g(x)}\neq 0 \;\middle|\; a_n b_t\text{ 为正实数}\right\}.$$

则 P_2 也给出 F 的一个序. 这是两个不同的序, 即 $P_1\neq P_2$. 例如 $\alpha=\dfrac{x-1}{x+1}$ 对于 P_1 为正元素, 而对于 P_2 为负元素. 事实上, 在域 $F=\mathbf{R}(x)$ 中存在无穷多个序: 设 c 为任意实数, $f(x)$ 为非零多项式, 则 $f(x)$ 可唯一地写成 $f(x)=(x-c)^n f_1(x)$, 其中 $f_1(x)$ 为多项式且 $f_1(c)\neq 0$(换句话说, c 不是多项式 $f_1(x)$ 的根, 即 c 为 $f(x)$ 的 n 重根, $n\geqslant 0$). 同样地, $g(x)=(x-c)^t g_1(x)$, $g_1(c)\neq 0$. 我们定义

$$P(a)=\left\{\alpha=\frac{f(x)}{g(x)}\neq 0 \;\middle|\; f_1(c)g_1(c)\text{ 为正实数}\right\}.$$

请大家证明 $P(a)$ 给出 $F=\mathbf{R}(x)$ 的一个序. 对于两个不同的实数 a 和 b, $P(a)$ 和 $P(b)$ 给出不同的序, 例如当 $a>b$ 时, $\alpha=x-a=\dfrac{x-a}{1}$ 属于 $P(a)$ 但不属于 $P(b)$. (为什么?)因此我们证明了 $\mathbf{R}(x)$ 中存在无穷多个序. 注意当 $a=0$ 时, $P(0)$ 即是前面的 P_2.

现在我们给出有序域的一些简单性质.

引理 1 设 F 是有序域, P 是定义序的正元集合, 则

(1) 对于每个 F 中非零元素 a, a^2 必是正元素.

(2) 1 必为正元素, -1 必为负元素.

(3) 若 $a>b$, $b>c$, 则 $a>c$.

(4) 若 $a>b$, $c>d$, 则 $a+c>b+d$.

(5) 若 $a>b$, $c>0$, 则 $ac>bc$.

若 $a>b$, $c<0$(即指 $0>c$), 则 $bc>ac$.

(特别地, 若 $a>b$, 则 $-b>-a$.)

证明 (1) 设 $a\neq 0$, 则 a 和 $-a$ 必有一个为正元素, 由于 $a^2=(-a)^2$, 从而 a^2 必是正元素的平方, 即 a^2 为正元素.

(2) $1=1^2\in P$, 而 $-1\in -P$.

(3) 若 $a>b$, $b>c$, 则 $a-b\in P$, $b-c\in P$, 于是 $a-c=(a-b)+(b-c)\in P$. 其余留给读者作练习.

练习 利用引理 1 的(1)证明实数域只有唯一的序.

引理 2 有序域必是形式实域.

证明 若 F 为有序域, 由引理 1 知对每个元素 $a\in F$, 必然 $a^2\geqslant 0$, 于是 $a_1^2+a_2^2+\cdots+a_n^2\geqslant 0$. 而 $-1<0$. 从而 -1 在 F 中不能是平方和, 即 F 是形式实域. 证毕.

由引理 2 可知 -1 在 $\mathbf{R}(x)$ 中也不是平方和, 因为例 2 表明 $\mathbf{R}(x)$ 是有序域. 下面我们要证明反过来也对, 即形式实域一定也是有序域, 也就是说: 如果 -1 不是域 F 中平方和, 则 F 中至少存在一个序. 这件事的证明则不显然了, 我们需要作一些准备.

今后以 $\sigma(F)$ 表示 F 中可表成平方和的元素全体, 即

$$\sigma(F)=\{a\in F\,|\,a \text{ 为 } F \text{ 中元素的平方和}\}.$$

如果 F 是有序域, 由引理 1 可知 $\sigma(F)$ 中每个非零元素对于 F 的每个序均为正元素. 下面引理表明集合 $\sigma(F)$ 对于域 F 中加、乘、除三种运算是封闭的.

引理 3 (1) 若 a, $b\in\sigma(F)$, 则 $a+b\in\sigma(F)$, $ab\in$

$\sigma(F)$. 又若 $b\neq 0$, 则 $\frac{a}{b}\in\sigma(F)$.

(2) 若 $-1\in\sigma(F)$, 则 $\sigma(F)=F$. 换句话说, 若 -1 为 F 中平方和(即 F 不是形式实域), 则 F 是每个元素均是 F 中平方和.

证明 (1) 若 $a=\sum_{i=1}^{n}a_i^2$, $b=\sum_{j=1}^{m}b_j^2$, 则

$$a+b=\sum_{i=1}^{n}a_i^2+\sum_{j=1}^{m}b_j^2,$$

$$ab=\sum_{i=1}^{n}\sum_{j=1}^{m}(a_ib_j)^2,$$

$$\frac{a}{b}=\frac{ab}{b^2}=\sum_{i=1}^{n}\sum_{j=1}^{m}\left(\frac{a_ib_j}{b}\right)^2.$$

(2) 设 a 为任意元素, 则

$$a=\left(\frac{a+1}{2}\right)^2-\left(\frac{a-1}{2}\right)^2=\left(\frac{a+1}{2}\right)^2+(-1)\left(\frac{a-1}{2}\right)^2.$$

由于 $\left(\frac{a+1}{2}\right)^2$, $\left(\frac{a-1}{2}\right)^2\in\sigma(F)$, 若假设 $-1\in\sigma(F)$, 则由(1)即知 $a\in\sigma(F)$, 于是 $\sigma(F)=F$. 证毕.

引理 4 设 F 为形式实域, $a\in F$, $a\notin\sigma(F)$, 则域 $F(\sqrt{-a})=\{A+B\sqrt{-a}\mid A,\ B\in F\}$ 仍是形式实域.

证明 若 $\sqrt{-a}\in F$, 则 $F(\sqrt{-a})=F$, 引理显然成立. 下设 $\sqrt{-a}\notin F$, 我们用反证法. 如果 $F(\sqrt{-a})$ 不是形式实域, 由定义知 $-1\in\sigma(F(\sqrt{-a}))$, 即 $-1=\sum_{i=1}^{n}(A_i+B_i\sqrt{-a})^2=\sum_{i=1}^{n}(A_i^2-aB_i^2)+2\sqrt{-a}\sum_{i=1}^{n}A_iB_i$, 其中 A_i, $B_i\in F$. 由 $\sqrt{-a}\notin F$ 可知 $\sum_{i=1}^{n}A_iB_i=0$, $-1=\sum_{i=1}^{n}A_i^2-a\sum_{i=1}^{n}B_i^2$. 如果 $\sum_{i=1}^{n}B_i^2=0$, 则 $-1=\sum_{i=1}^{n}A_i^2\in\sigma(F)$, 这与 F 为形式实域相矛盾. 因此 $\sum_{i=1}^{n}B_i^2\neq 0$, 于是 $a=(1+\sum_{i=1}^{n}A_i^2)/\sum_{i=1}^{n}B_i^2$. 由引理 3 的

(1)即知 $a\in\sigma(F)$. 因此当 $a\notin\sigma(F)$时, $F(\sqrt{-a})$ 为形式实域. 证毕.

现在我们证明

引理 5 每个形式实域均是有序域.

证明 设 F 是形式实域. 如果 $a\notin\sigma(F)$并且 $\sqrt{-a}\notin F$,由引理 4 知 $F(\sqrt{-a})$仍是形式实域. 对于 F 中所有元素 $b\notin\sigma(F)$,均把 $\sqrt{-b}$ 按上述办法加到 F 中,便可作成一个域

$$F_1=F(\sqrt{-b}\,|\,b\in F,\ b\notin\sigma(F)).$$

F_1 仍为形式实域. 如果 F_1 中又有元素 $a_1\notin\sigma(F_1)$, 我们再把这些 $\sqrt{-a_1}$ 加到 F_1 中得到更大的域 F_2, 如此进行下去, 最后便得到一个形式实域 E,使得 E 按上述方式不能再扩大了, 即 E 有以下特性: 对每个 $a\in E$, 如果 $a\notin\sigma(E)$, 则必然 $\sqrt{-a}\in E$. (注意: 上面所讲域 E 的存在性只是一种形象的描述,在数学上是不严格的. 为了严格证明域 E 的存在性, 需要所谓"超限归纳法", 这是比大家熟知的数学归纳法更为高级的手段. 我们不想再讲什么是超限归纳法, 只想告诉大家,具有上述性质的 F 的扩域 E 是存在的.)

我们要证 E 是有序域(由此立刻推出其子域 F 也是有序域, 即证明了引理 5). 为此我们首先证明: 对于 E 中每个非零元素 x, 在 $\pm x$ 当中恰有一个是 E 中元素的平方. 这是由于 E 为形式实域, 因此 -1 不是 E 中元素的平方, 从而 $\pm x$ 至多有一个是 F 中元素的平方. 进而若 x 是 E 中平方元素, 则 $-x$ 不是平方元素. 若 x 和 $-x$ 都不是 E 中平方元素, 即 $\sqrt{-x}, \sqrt{x}\notin E$. 由 E 的上述特性可知 $\pm x\in\sigma(E)$, 于是 $-1\in\sigma(F)$, 这又与 E 是形式实域相矛盾. 因此对 E 中每个非零元素 x, x 和$(-x)$恰有一个是 E 中平方元素. 如

果以 P 表示 E 中全体非零元素的平方构成的集合，上述命题表明 P 和集合 $-P$ 不相交，并且 E 恰好是$\{0\}$, P 和 $-P$ 的并集．并且 P 中可作加法和乘法(若 x, $y\in P$, 即 $x=a^2$, $y=b^2$, a, $b\in E$, 则 $xy=(ab)^2\in P$. 而 $x+y=a^2+b^2$ 也是平方元素．因若 $a^2+b^2\notin P$,则或者 $a^2+b^2\in -P$,于是 $a^2+b^2=-c^2\neq 0$, $c\in E$. 从而 $-1=\left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2\in\sigma(F)$；或者 $a^2+b^2=0$, 由于 $x=a^2\in P$, 从而 $a\neq 0$, $-1=\left(\frac{b}{a}\right)^2\in\sigma(F)$. 这均与 E 为形式实域相矛盾)．这就证明了 P 满足定义序的两个条件，从而 E 是有序域．这就证明了引理 5.

由引理 2 和引理 5 可知，一个域是形式实域，当且仅当它是有序域．换句话说，-1 在域 F 中是平方和，当且仅当域 F 中不存在序(由引理 3 的(2)可知这又等价于：F 中每个元素均是平方和)．由于形式实域和有序域这两个概念是同样的事情，今后我们只把它叫作有序域．例如，我们可以把引理 4 叙述成：若 F 是有序域，$a\notin\sigma(F)$, 则 $F(\sqrt{-a})$ 也是有序域。

2. 全正元素是平方和

我们在前小节证明了，若 F 没有序，即 $-1\in\sigma(F)$，则 F 中所有元素均为平方和，即 $\sigma(F)=F$. 如果 F 是有序域，则 $-1\notin\sigma(F)$．那么，F 中哪些元素是平方和呢？即 $\sigma(F)=$？本小节我们研究这问题.

定义 设 $a\in F$, a 叫作 F 的全正元素，是指对于 F 的每个序，a 均是正元素．注意若 F 不是有序域，则我们自然规定 F 中所有非零元素均是全正元素。

定理1 设$a\in F$, $a\neq 0$, 则$a\in\sigma(F)$当且仅当a是F的全正元素.

证明 若F不是有序域,则$\sigma(F)=F$,而所有非零元素均是全正的,于是定理成立. 若F是有序域, $a\in F$, $a\neq 0$. 如果$a\in\sigma(F)$,即a是F中元素的平方和,显然对F中每个序,a均是正元素. 因此a是全正的. 反之若$a\notin\sigma(F)$,则由引理4知$F(\sqrt{-a})$也是有序域.设P是域$F(\sqrt{-a})$对于某个序的正元集合,则由第一小节例1末尾所述,集合$P'=P\cap F$给出域F的一个序.由于$-a=(\sqrt{-a})^2\in P$, 并且$a\in F$,从而$-a\in P\cap F=P'$.即$-a$为F中上述序的正元素,从而a对于F的上述序为负元素. 这就表明a不是F中全正元素. 证毕.

这个定理在理论上是很漂亮的. 但是事实上判别有序域F中某个非零元素a是否为平方和时,即a是否为全正元素时,我们往往需要知道域F的所有序,然后检验a对每个序是否均是正元素. 而在一般情形下,要决定域F的所有序是困难的. 现在我们就数论上非常有用的一类域进行进一步的讨论.

我们以$\mathbf{Q}$表示有理数域. 由于$-1\notin\sigma(\mathbf{Q})$, 从而$\mathbf{Q}$是有序域.事实上, $\mathbf{Q}$中只有一个序,即通常意义下的序. 因为设$\mathbf{Q}$中任给了一个序,令P为$\mathbf{Q}$中对此序的正元素集合,则$1\in P$(引理1), 从而对每个正整数m, $m=1+1+\cdots+1$(m个)$\in P$.于是对任意两个正整数m, n, $\frac{m}{n}=mn\cdot\left(\frac{1}{n^2}\right)\in P$. 这就表明所有正有理数对于由$P$给的序均是正元素,而所有负有理数均是负元素, 所以由P给出的序就是通常的序, 即$\mathbf{Q}$中只有唯一的序.

以 $\mathbf{Q}[x]$ 表示关于 x 的有理系数多项式全体.这个集合对于通常的多项式加法和乘法运算形成一个环，叫作 $\mathbf{Q}$ 上的多项式环. 像第二节最后一小节对高斯整数环 $\mathbf{Z}[i]$ 所作的那样，我们也可以定义环 $\mathbf{Q}[x]$ 中的整除性概念、(乘法)可逆元概念等等.设 $f(x)$ 和 $g(x)$ 是 $\mathbf{Q}[x]$ 中两个多项式，$g(x)\neq 0$.如果 $f(x)/g(x)$ 是多项式，则称 $g(x)$ 整除 $f(x)$，表示成 $g(x)\mid f(x)$.并且称 $g(x)$ 是 $f(x)$ 的因子.如果 $\frac{1}{g(x)}$ 仍是多项式，则称 $g(x)$ 是可逆元.

设多项式 $g(x)\neq 0$ 是环 $\mathbf{Q}[x]$ 中可逆元，则 $h(x)=\frac{1}{g(x)}$ 为多项式. 于是 $g(x)h(x)=1$. 设 $g(x)$ 和 $h(x)$ 的多项式次数为 n 和 m，则 $g(x)h(x)$ 的次数为 $m+n$. 而多项式 1 的次数为零. 因此 $m+n=0$. 从而必然 $m=n=0$，即 $g(x)$ 和 $h(x)$ 均为零次多项式，即 $g(x)$ 为非零有理数. 反之，若 $g(x)=a$，a 为非零有理数，则 $\frac{1}{g(x)}=a^{-1}\in\mathbf{Q}\subseteq\mathbf{Q}[x]$，从而 $g(x)$ 可逆.这就表明，环 $\mathbf{Q}[x]$ 的可逆元全体恰好为全部非零有理数. 所以环 $\mathbf{Q}[x]$ 中有无穷多个可逆元.

接下来应当定义环 $\mathbf{Q}[x]$ 中两个多项式的等价概念. 与高斯整数环 $\mathbf{Z}[i]$ 的情形相仿，对于两个非零多项式 $f(x)$，$g(x)\in\mathbf{Q}[x]$，称 $f(x)$ 和 $g(x)$ 等价，是指存在可逆元(即非零有理数)a，使得 $g(x)=af(x)$，并且表示成 $f(x)\sim g(x)$.于是，$\mathbf{Q}[x]$ 中所有非零多项式分拆成许多等价类，同一等价类中的多项式彼此相差一个非零有理数因子. 设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n(a_i\in\mathbf{Q})$ 是某个非零多项式，$a_0\neq 0$(于是 f 的次数为 n)，则首项系数为 1 的多项式 $x^n+\frac{a_1}{a_0}x^{n-1}+\cdots+\frac{a_n}{a_0}$

与 f 等价，并且不难看出，每个等价类中恰好有一个首项系数为 1 的多项式，我们自然取它为该等价类中的代表元.

再下来我们应当弄清 $\mathbf{Q}[x]$ 中哪些多项式相当于通常整数环中的素数或高斯整数环中的高斯素数. 一个高斯整数 α 叫作是高斯素数，是指 α 的因子或者为可逆元，或者与 α 等价. 类似地，我们也应当考虑 $\mathbf{Q}[x]$ 中那些多项式 $f(x)$，使得 $f(x)$ 的因子或者为可逆元(即非零有理数)，或者与 $f(x)$ 等价. 这也相当于说 $f(x)$ 不能分解成两个有理系数多项式 $g(x)$ 和 $h(x)$ 之积，使得 $g(x)$ 和 $h(x)$ 的次数均小于 $f(x)$ 的次数(请大家证明这件事). 这样的多项式通常叫作是($\mathbf{Q}$ 上)不可约多项式. 所以，不可约多项式的作用相当于"素数"的作用.

有了以上这些概念之后，我们要证明 $\mathbf{Q}[x]$ 也有素因子唯一分解性质. 我们证明高斯整数环 $\mathbf{Z}[i]$ 具有素因子唯一分解性质，是基于 $\mathbf{Z}[i]$ 中有除法算式(第二节引理 10 的(1)). 我们在中学里学过环 $\mathbf{Q}[x]$ 中也有下面类似的除法算式(只不过用"多项式次数"来代替"高斯整数的范")：

设 $f(x), g(x)\in\mathbf{Q}[x]$, $g(x)\neq 0$. 则存在 $q(x), r(x)\in\mathbf{Q}[x]$，使得 $f(x)=q(x)g(x)+r(x)$，并且或者 $r(x)=0$，或者 $r(x)$ 的次数小于 $g(x)$ 的次数.

有了除法算式，我们可以类似地证明像第二节引理 9 的(2)那样的命题(读者作为练习)：

设 $f(x), g(x)$ 为两个非零有理系数多项式，并且 $f(x)$ 和 $g(x)$ 互素(即它们没有次数 $\geqslant 1$ 的有理系数多项式公因子)，则存在 $h(x), l(x)\in\mathbf{Q}[x]$，使得 $f(x)h(x)+g(x)l(x)=1$.

然后可以完全一样地证明(读者自证)：

环 $\mathbf{Q}[x]$ 的素因子唯一分解性质 $\mathbf{Q}[x]$ 中每个次数大于 1 的多项式 $f(x)$ 均可表成有限个不可约多项式之乘积；

$f(x)=p_1(x)p_2(x)\cdots p_t(x)$. 其中 $p_i(x)$ 均是 $\mathbf{Q}[x]$ 中不可约多项式. 并且,若又有 $f(x)=q_1(x)\cdots q_s(x)$,其中 $q_i(x)$ 也均是 $\mathbf{Q}[x]$ 中不可约多项式, 则 $t=s$, 并且适当调整 $q_i(x)$ 的下标, 可使 $p_i(x)\sim q_i(x)\ (1\leqslant i\leqslant t)$.

设 $f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ 是 $\mathbf{Q}[x]$ 中首项系数为 1 的不可约多项式. 由代数基本定理, 我们知道方程 $f(x)=0$ 在复数域 $\mathbf{C}$ 中恰好有 n 个根: $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n$. 由于 $f(x)$ 不可约, 可知 $f(x)=0$ 没有重根, 即 $\alpha_1,\ \cdots,\ \alpha_n$ 彼此不同. 设 α 为其中任意一个根.

引理 6 集合 $K=\mathbf{Q}[\alpha]=\{c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}|c_0,\ \cdots,\ c_{n-1}\in\mathbf{Q}\}$ 是域. 并且 K 中每个数可唯一表成 $c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}$(其中 $c_0,\ \cdots,\ c_{n-1}\in\mathbf{Q}$).

证明 对于 K 中两个数 $A=c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}$, $B=d_0+d_1\alpha+\cdots+d_{n-1}\alpha^{n-1}$,其中 $c_i,\ d_i\in\mathbf{Q}$, 显然 $A\pm B=(c_0\pm d_0)+(c_1\pm d_1)\alpha+\cdots+(c_{n-1}\pm d_{n-1})\alpha^{n-1}\in K$. 又令 $g(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$, $h(x)=d_0+d_1x+\cdots+d_{n-1}x^{n-1}$. 由除法算式知存在 $q(x)$ 和 $r(x)\in\mathbf{Q}[x]$, 使得 $g(x)h(x)=q(x)f(x)+r(x)$,并且 $r(x)\equiv0$ 或者 $r(x)$ 的次数小于 $f(x)$ 的次数 n. 令 $r(x)=r_0+r_1x+\cdots+r_{n-1}x^{n-1}$, 其中 $r_i\in\mathbf{Q}$. 于是 $AB=g(\alpha)h(\alpha)=q(\alpha)f(\alpha)+r(\alpha)=r(\alpha)$ (因为 $f(\alpha)=0$) $=r_1+r_1\alpha+\cdots+r_{n-1}\alpha^{n-1}\in K$. 最后再证 K 中可作除法. 设 $B\neq0$, 于是 $h(x)$ 不恒为 0. 我们只需证明 $B^{-1}\in K$ 即可, 由于 $h(x)$ 的次数小于 $f(x)$ 的次数 n, 并且 $f(x)$ 不可约, 从而 $h(x)$ 与 $f(x)$ 互素. 于是存在 $k(x)$, $l(x)\in\mathbf{Q}[x]$, 使得 $h(x)k(x)+l(x)f(x)=1$. 因此 $1=h(\alpha)k(\alpha)+l(\alpha)f(\alpha)=B\cdot k(\alpha)$. 令 $k(x)=e_0+e_1x+\cdots+e_mx^m$, $e_i\in\mathbf{Q}$. 则 $k(\alpha)=e_0+e_1\alpha+\cdots+e_m\alpha^m$. 我们已经证明了 K 中可作加法和乘法. 再由 $e_i\in\mathbf{Q}\subseteq$

K 和 $\alpha\in K$ 便知 $h(\alpha)\in K$. 于是由 $B\cdot h(\alpha)=1$ 可知 B 在 K 中可逆. 这就证明了 K 中每个非零数均可逆, 从而 K 为域.

设 $A=c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}=c_0'+c_1'\alpha+\cdots+c_{n-1}'\alpha^{n-1}$, 其中 c_i, $c_i'\in\mathbf{Q}$. 则 $(c_0-c_0')+(c_1-c_1')\alpha+\cdots+(c_{n-1}-c_{n-1}')\alpha^{n-1}=0$. 令 $g(x)=(c_0-c_1')+(c_1-c_1')x+\cdots+(c_{n-1}-c_{n-1}')x^{n-1}$, 则 $g(\alpha)=0$. 如果 $g(x)$ 不恒等于 0, 则由于 $g(x)$ 的次数小于 $f(x)$ 的次数 n, 并且 $f(x)$ 不可约, 可知 $g(x)$ 与 $f(x)$ 互素. 于是有 $h(x)$, $l(x)\in\mathbf{Q}[x]$, 使得 $f(x)h(x)+g(x)l(x)=1$. 从而 $1=f(\alpha)h(\alpha)+g(\alpha)l(\alpha)=0\cdot h(\alpha)+0\cdot l(\alpha)=0$, 这就导致矛盾, 所以必然 $g(x)$ 恒等于 0, 即 $c_0=c_0'$, $c_1=c_1'$, $\cdots$, $c_{n-1}=c_{n-1}'$. 这就证明了表达式的唯一性. 证毕.

引理 6 中的域 K 叫作代数数域. 其 α 所满足的不可约多项式 $f(x)$ 的次数也叫作域 K 的次数. 即 K 叫做 n 次代数数域, 或简称 n 次域. 研究代数数域的性质便是代数数论的主要任务.

现在我们看看代数数域有哪些序. 设 K 是代数数域, $K=\mathbf{Q}[\alpha]$, 其中 α 是某个 n 次不可约多项式 $f(x)\in\mathbf{Q}[x]$ 的根. 设 $f(x)$ 的所有 n 个根为 α_1, $\cdots$, α_n (当然 α 是其中之一).

(1) 如果 α_1, $\cdots$, α_n 均不是实数, 可以证明 K 不是有序域 (从而 K 中每个元素均是平方和).

(2) 设 α_1, $\cdots$, α_t 是实数 $(t\geqslant 1)$, 而 α_{t+1}, $\cdots$, α_n 不是实数, 则 K 中每个非零元素均可唯一表成 $A=c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}$ $(c_i\in\mathbf{Q})$. 对于每个 i $(1\leqslant i\leqslant t)$, 由引理 6 知 $K_i=\mathbf{Q}[\alpha_i]=\{a_0+a_1\alpha_i+\cdots+a_{n-1}\alpha_i^{n-1}\mid a_i\in\mathbf{Q}\}$ 均是域. 由于 $A\neq 0$, 从而 c_0, $\cdots$, c_{n-1} 不全为 0 (引理 6), 于是 $A_i=c_0+c_1\alpha_i+\cdots+c_{n-1}\alpha_i^{n-1}\neq 0$. 由于 α_i 为实数, 从而 A_i 为非零实数. 令

$P_i=\{A=c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}\in K=\mathbf{Q}[\alpha]\mid A_i=c_0+c_1\alpha_i+\cdots+c_{n-1}\alpha_i^{n-1}$为正实数$\}$. 请读者证明$P_i$具有定义序的那两条性质, 即(1) K分拆成三个彼此不相交集合$\{0\}$, P_i和$-P_i$的并集. (2)若A, $B\in P_i$, 则$A+B$, $AB\in P_i$. 于是由P_i决定出域K的一个序. 这就表明: 若$f(x)=0$有实根, 则K必是有序域. 特别地, 若$f(x)$是奇次多项式, 熟知$f(x)$必有实根. 从而奇次代数数域必是有序域(因此在奇次代数数域中, -1不是平方和).

可以证明: 集合$P_i(1\leqslant i\leqslant t)$给出域$K$的$t$个不同的序, 并且$K$恰好只有这$t$个序. 因此, K中元素A是全正元素(即A在K中为平方和), 当且仅当A_1, A_2, $\cdots$, A_t均是正实数. 这就给出代数数域K中判别哪些元素可表成平方和的一个切实有效的判别法.

【例1】 设$K=\mathbf{Q}(\sqrt{-2})$. 则$\sqrt{-2}$是多项式$x^2+2\in\mathbf{Q}[x]$的根, 易知x^2+2在$\mathbf{Q}$上是不可约的. 因为若它可约, 则必可写成两个一次多项式之积, 即$x^2+2=(x-\alpha)(x-\beta)$, 其中$x-\alpha$, $x-\beta\in\mathbf{Q}[x]$, 于是α, $\beta\in\mathbf{Q}$. 从而x^2+2有两个有理数的根. 但是$x^2+2=0$的两个根$\pm\sqrt{-2}$均不是有理数. 因此x^2+2在$\mathbf{Q}$上不可约. 由于x^2+2没有实根, 由前面所述, 便知$K=\mathbf{Q}(\sqrt{-2})$不是有序域. 所以K中每个元素均是平方和.

(或者用下面方法可以更简单地看出K不是有序域: 由于$-1=1^2+(\sqrt{-2})^2$, 即-1为K中平方和, 从而K不是有序域.)

【例2】 设$f(x)=x^3+x+1$, 我们先证明$f(x)$为$\mathbf{Q}$上不可约多项式. 如果$f(x)$在$\mathbf{Q}$上可约, 由于$f(x)$的次数为3, 则$f(x)$必有一次因子$x-a$, $a\in\mathbf{Q}$. 即$f(x)$必有有理数a为

根．设 $a=\frac{n}{m}$，其中 n 和 m 均为整数，$m\neq 0$，并且不妨设 n 和 m 互素，于是 $\left(\frac{n}{m}\right)^3+\left(\frac{n}{m}\right)+1=0$，即 $n^3+nm^2+m^3=0$．于是 $n^3=-m^2(n+m)$，从而 $m\mid n^3$．由于 m 和 n 互素，必然 $m=\pm 1$，因此 a 为整数．由 $a^3+a+1=0$，即知 $a(a^2+1)=-1$．由于 a 和 a^2+1 均为整数，可知 $a=\pm 1$．但是 $f(1)=3$，$f(-1)=-1$，所以 $f(x)$ 没有有理数根．即 $f(x)$ 在 $\mathbf{Q}$ 上不可约．

由于 $f(x)$ 是奇次多项式，所以它至少有一个实根 α．于是 $f(x)=x^3+x+1=(x-\alpha)(x^2+\alpha x+(1+\alpha^2))$．由于 $x^2+\alpha x+(1+\alpha^2)$ 的判别式 $\alpha^2-4(1+\alpha^2)=-4-3\alpha^2<0$，可知 $x^2+\alpha x+(1+\alpha^2)$ 没有实根．这就表明 $f(x)$ 的三个根 α_1，α_2，α_3 当中恰好有一个为实根 α．

以 β 表示 $f(x)$ 的三个根 α_1，α_2，α_3 当中的任何一个．令 $K=\mathbf{Q}[\beta]=\{c_0+c_1\beta+c_2\beta \mid c_0, c_1, c_2\in\mathbf{Q}\}$，这是三次代数数域．当 $\beta=\alpha$ 时，$K=\mathbf{Q}[\alpha]$ 中所有数都是实数，K 作为实数域的子域，当然是有序域．但是由上面的结论我们知道，即使 β 是（除 α 之外）另外两个非实根时，尽管此时 $K=\mathbf{Q}[\beta]$ 不包括在实数域之中，K 仍然有序，并且对于 β 为三个根当中任何一个的时候，$K=\mathbf{Q}[\beta]$ 均只有一个序（因为 $f(x)$ 只有一个实根 α），这个序就是：对每个 K 中非零元素 $A=c_0+c_1\beta+c_2\beta^2$ $(c_0, c_1, c_2\in\mathbf{Q})$，则 A 为正元素 $\Leftrightarrow$ $c_0+c_1\alpha+c_2\alpha^2$ 为正实数．由于 K 中只有一个序，从而 K 中非零元素 $A=c_0+c_1\beta+c_2\beta^2$ 是全正元素（即 A 为 K 中平方和）当且仅当 $c_0+c_1\alpha+c_2\alpha^2$ 为正实数．

【例 3】 $K=\mathbf{Q}[\sqrt{2}]$．由于 $\sqrt{2}$ 是不可约多项式 $x^2-2\in\mathbf{Q}[x]$ 的根，面 x^2-2 有两个实根 $\pm\sqrt{2}$，从而 $K=$

$\mathbf{Q}[\sqrt{2}]$有两个序. 一个序为: $a+b\sqrt{2}$ $(a, b\in\mathbf{Q})$ 是正元素 $\leftrightarrow a+b\sqrt{2}>0$; 另一个序为: $a+b\sqrt{2}$ 是正元素 $\leftrightarrow a+b(-\sqrt{2})=a-b\sqrt{2}>0$. 从而: K 中元素 $a+b\sqrt{2}$ $(a,b\in\mathbf{Q})$是全正的(即 $a+b\sqrt{2}$ 是 $\mathbf{Q}[\sqrt{2}]$中平方和)当且仅当 $a+b\sqrt{2}$ 和 $a-b\sqrt{2}$ 均为正实数.

例如: $2+\sqrt{2}$ 是域 $\mathbf{Q}[\sqrt{2}]$中平方和, 因为 $2+\sqrt{2}$ 和 $2-\sqrt{2}$ 均为正实数. 而 $1+\sqrt{2}$ 不是域 $\mathbf{Q}[\sqrt{2}]$中全正元素, 因为 $1-\sqrt{2}<0$, 即 $1+\sqrt{2}$ 对于域 $\mathbf{Q}[\sqrt{2}]$的第二个序是负元素. 所以, 尽管 $1+\sqrt{2}>0$, 但是 $1+\sqrt{2}$不是域 $\mathbf{Q}[\sqrt{2}]$中的平方和.

3. −1是几个数的平方和——虚二次域情形

我们在第 3.1 小节证明了 -1 为域 F 中平方和的充分必要条件是 F 中没有序. 在第 3.2 小节我们又介绍了一个代数数域中何时 -1 为平方和: 设代数数域 $K=\mathbf{Q}[\alpha]$, 其中 α 是某个 n 次不可约多项式 $f(x)\in\mathbf{Q}[x]$的根, 则 -1 为 K 中平方和的充分必要条件是 $f(x)$没有实根. 现在我们进一步问: 如果 -1 是某个域 F 中的平方和, 那么 -1 在 F 中最少可以表成几个数的平方和? 本小节中我们对 F 是虚二次域的情形研究这个问题.

我们从前小节知道, 所谓二次域即指域 $K=\mathbf{Q}[\alpha]$, 其中 α 是不可约二次多项式 $f(x)=x^2+ax+b\in\mathbf{Q}[x]$ 的根. 由于 $x^2+ax+b=\left(x+\frac{a}{2}\right)^2+\left(b-\frac{a^2}{4}\right)$, 令 $g(y)=y^2-\left(b-\frac{a^2}{4}\right)$, 若 α 为 $f(x)$的根, 则 $\alpha+\frac{a}{2}$ 为 $g(y)$的根. 由于 $\frac{a}{2}$ 是有理数,

易知域$\mathbf{Q}[\alpha]$和$\mathbf{Q}\left[\alpha+\frac{a}{2}\right]$是一回事(请读者自证). 因此我们不妨设二次不可约多项式有形式 $f(x)=x^2-a$, 其中 a 为有理数, 而 $f(x)$不可约相当于说 a 不是有理数的平方. 这时 $K=\mathbf{Q}[\sqrt{a}]$. 设 $a=\frac{m}{n}$, 其中 m, n 均为整数, $n\neq 0$. 则 $\sqrt{a}=\sqrt{\frac{m}{n}}=\frac{1}{n}\sqrt{mn}$, 易知$\mathbf{Q}(\sqrt{a})=\mathbf{Q}\left(\frac{1}{n}\sqrt{mn}\right)$和域$\mathbf{Q}(\sqrt{mn})$是一回事. 从而我们又不妨设 a 为整数(并且不是完全平方数). 设 $a=m^2m'$, 其中 m' 是整数 a 的无平方因子部分, 则 $\sqrt{a}=m\sqrt{m'}$, 而$\mathbf{Q}(\sqrt{a})=\mathbf{Q}(\sqrt{m'})$. 所以最后我们知道每个二次域总可写成$K=\mathbf{Q}(\sqrt{a})$, 其中 a 是整数, $\sqrt{a}\notin\mathbf{Z}$, 并且 a 没有平方因子.

当 $a>0$ 时, $\sqrt{a}$ 为实数, 从而 $K=\mathbf{Q}(\sqrt{a})$中所有数 $A=c_0+c_1\sqrt{a}$ $(c_0, c_1\in\mathbf{Q})$均是实数, 这时称 K 为实二次域. 当 $a<0$ 时, K 叫作虚二次域. 这时方程 $x^2-a=0$ 的两个根 $\pm\sqrt{a}$ 均不是实数. 所以虚二次域不是有序域, 因此 -1 在任意虚二次域中均可表为平方和. 事实上, 这件事可以很容易看出: 因为设 $a=-n$, 其中 n 为正整数, 则 $-1=\underbrace{1^2+1^2+\cdots+1^2}_{(n-1)\text{个}}+(\sqrt{a})^2$, 即 -1 在虚二次域$\mathbf{Q}(\sqrt{-n})$中可表成 n 个数的平方和. 问题在于: -1 能否表成更少个数的平方和?所需最少的数是多少?

一般地, 我们设 F 是没有序的, 并且以 $s(F)$表示最小正整数 n, 使得 -1 为 F 中 n 个数的平方和. 当 F 没有序时, -1 总可表成 F 中数的平方和, 从而最小可能的 n 值是存在的. 对于虚二次域 $K=\mathbf{Q}(\sqrt{-n})$, 我们在上面已知 $s(K)\leqslant n$. 事实上, 对于虚二次域我们可以算出 $s(K)$的确切值来. 而

且有趣的是：这个问题与第一节关于正整数表成平方和问题有非常密切的关系．确切地说，我们在本小节中要证明下面有趣的定理：

定理 2 设 m 是无平方因子的正整数，$K=\mathbf{Q}(\sqrt{-m})$．则

$$s(K)=\begin{cases}1, & \text{如果 } m=1;\\ 2, & \text{如果 } m\neq 1, \text{并且 } m\not\equiv 7 \pmod 8;\\ 4, & \text{如果 } m\equiv 7 \pmod 8).\end{cases}$$

从第一节的结果我们可将此定理改说成：$s(K)=1\Leftrightarrow m$ 是（整数的）一平方（和）；$s(K)=2\Leftrightarrow m$ 是三平方和但不是一平方（和）；$s(K)=4\Leftrightarrow m$ 是四平方和但不是三平方和．

为了证明这个定理，我们先作一点准备．

引理 7 若正整数 n 是三个有理数的平方和，则 n 也是三个整数的平方和．

证明 设 $n=\alpha^2+\beta^2+\gamma^2$，其中 α, β, γ 均为有理数．我们将 α, β, γ 写成分数形式，令 N 是它们分母的最小公倍数，则总可写成 $\alpha=\frac{a}{N}$，$\beta=\frac{b}{N}$，$\gamma=\frac{c}{N}$，其中 N 是正整数，而 a, b, c 为整数．于是 $nN^2=a^2+b^2+c^2$，即 nN^2 可表成三整数平方和．令 $N=2^\alpha\cdot M$，其中 M 为奇数．而令 $n=4^\beta\cdot m$，其中 $4\nmid m$．则 $nN^2=4^{\alpha+\beta}M^2m$．由于 M 为奇数，从而 $4\nmid M^2m$，并且因为 $M^2\equiv 1 \pmod 8$，可知 $M^2m\equiv m \pmod 8$．由于 nN^2 为三整数平方和，根据第一节关于三平方和的高斯定理，可知 $M^2m\not\equiv 7 \pmod 8$，于是 $m\not\equiv 7 \pmod 8$．再应用这个定理即知 n 为三整数平方和．证毕．

引理 8 设 F 为任一域，则 -1 为 F 中 n 平方和 $\Leftrightarrow$ 方程 $x_1^2+x_2^2+\cdots+x_{n+1}^2=0$ 在 F 中有非零解（即存在不全为零

的 F 中元素 $a_1, \cdots, a_{n+1}$, 使 $a_1^2+\cdots+a_{n+1}^2=0$).

证明 若 $-1=c_1^2+\cdots+c_n^2$, $c_i\in F$, 则 $(a_1, \cdots, a_{n+1})=(c_1, \cdots, c_n, 1)$ 便是方程 $x_1^2+\cdots+x_{n+1}^2=0$ 的非零解. 反之, 若 $a_1^2+\cdots+a_{n+1}^2=0$, 其中 $a_1, \cdots, a_{n+1}\in F$ 并且不全为零. 不妨设 $a_{n+1}\neq 0$, 则 $-1=\left(\frac{a_1}{a_{n+1}}\right)^2+\cdots+\left(\frac{a_n}{a_{n+1}}\right)^2$. 证毕.

引理9 设 F 为任一域. 若 $s(F)\leqslant 3$, 则 $s(F)\leqslant 2$.

证明 设 $-1=a^2+b^2+c^2$, $a, b, c\in F$. 如果 $1+a^2=0$, 则 $-1=a^2$, 于是 $s(F)=1$, 证毕. 若 $1+a^2\neq 0$. 请直接验证 $-1=\left(\frac{b-ac}{1+a^2}\right)^2+\left(\frac{c+ab}{1+a^2}\right)^2$, 于是 $s(F)\leqslant 2$. 证毕.

注记. 也许大家不知上面 -1 表成二平方和的公式是怎么得来的. 现在给出一个更容易理解的证明. 仍设 $1+a^2\neq 0$. 则由 $-1=a^2+b^2+c^2$ 得到 $-(1+a^2)=b^2+c^2$. 于是 $-1=\frac{b^2+c^2}{1+a^2}=\frac{(b^2+c^2)(1+a^2)}{(1+a^2)^2}=\left[\left(\frac{b}{d}\right)^2+\left(\frac{c}{d}\right)^2\right](1+a^2)$, 其中 $d=1+a^2\neq 0$. 但是我们已经知道两个二平方和之积仍是二平方和, 这就证明了定理. 如果我们将上式具体使用恒等式 $(x^2+y^2)(z^2+w^2)=(xz-yw)^2+(xw+yz)^2$, 便自然得到引理9证明中那个将 -1 具体表成二平方和的式子.

现在我们可以证明定理2.

(1) 若 $m=1$, 则 $\sqrt{-1}\in K$, $-1=(\sqrt{-1})^2$, 从而 $s(K)=1$. 反之若 $s(K)=1$, 则 $-1=(a+b\sqrt{-m})^2=a^2-mb^2+2ab\sqrt{-m}$ $(a, b\in \mathbf{Q})$. 由于域 $K=\mathbf{Q}(\sqrt{-m})$ 中每个数表示成 $c+d\sqrt{-m}$ $(c, d\in \mathbf{Q})$ 是唯一的, 因此必然 $-1=a^2-mb^2$, $ab=0$. 若 $b=0$, 则 $-1=a^2$, 这显然不可能. 因此 $a=0$; 于是 $-1=-mb^2$, 即 $mb^2=1$. 由于 m 是无平方因子的正整数, 从而只能 $b=\pm 1$, $m=1$. 这就证明了: $s(K)=1\Leftrightarrow m=1$.

下设 $m\geqslant 2$，于是 $s(K)\geqslant 2$.

(2) 我们再证：m 为三整数平方和(这又相当于 $m\not\equiv 7 \pmod 8$)$\Leftrightarrow s(K)\leqslant 3$ (由引理 9 知这又相当于 $s(K)=2$). 首先，若 $m=a^2+b^2+c^2$，$a, b, c\in\mathbf{Z}$，则 $0=a^2+b^2+c^2+(\sqrt{-m})^2$. 由引理 8 可知 -1 在 K 中为三平方和，即 $s(K)\leqslant 3$. 反之，若 $s(K)\leqslant 3$，则由引理 8 知存在 a_i, $b_i(1\leqslant i\leqslant 4)\in\mathbf{Q}$，并且 a_i, b_i 不全为零，使得

$$
\begin{aligned}
0&=\sum_{i=1}^{4}(a_i^2+b_i^2\sqrt{-m})\\
&=\left(\sum_{i=1}^{4}a_i-m\sum_{i=1}^{4}b_i\right)+2\left(\sum_{i=1}^{4}a_ib_i\right)\sqrt{-m}.
\end{aligned}
$$

因此 $\sum\limits_{i=1}^{4}a_i^2=m\sum\limits_{i=1}^{4}b_i^2, \sum\limits_{i=1}^{4}a_ib_i=0$. 如果 $b_i(1\leqslant i\leqslant 4)$ 均为零，则 $\sum\limits_{i=1}^{4}a_i^2=m\sum\limits_{i=1}^{4}b_i^2=0$，从而 $a_i(1\leqslant i\leqslant 4)$ 也均为零，这与 a_i, b_i 不全为零矛盾. 从而 $b_i(1\leqslant i\leqslant 4)$ 不全为零，于是 $\sum\limits_{i=1}^{4}b_i\neq 0$，从而 $m\left(\sum\limits_{i=1}^{4}b_i^2\right)^2=\left(\sum\limits_{i=1}^{4}a_i\right)\left(\sum\limits_{i=1}^{4}b_i\right)$. 现在我们利用第一节中关于两个四平方和之积仍是四平方和的恒等式：

$$
\begin{aligned}
&(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)\\
&\quad=(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+B^2+C^2+D^2,
\end{aligned}
$$

可知 $m\left(\sum\limits_{i=1}^{4}b_i^2\right)^2=\left(\sum\limits_{i=1}^{4}a_ib_i\right)^2+B^2+C^2+D^2$. 但是 $\sum\limits_{i=1}^{4}a_ib_i=0$，于是 $m\left(\sum\limits_{i=1}^{4}b_i^2\right)^2$ 是三个有理数平方和，从而 m 也是三个有理数平方和. 再由引理 7 可知 m 为三整数平方和. 这就证明了：当 $m\neq 1$，$m\not\equiv 7 \pmod 8$ 时 $s(K)=2$.

(3) 现设 $m\equiv 7 \pmod 8$. 则由(2)可知 $s(K)\geqslant 4$. 我们只需再证 $s(K)\leqslant 4$. 这是由于 m 为四整数平方和，$m=a^2+b^2+c^2+d^2$，$a, b, c, d\in\mathbf{Z}$，于是

$$0=a^2+b^2+c^2+d^2+(\sqrt{-m})^2.$$

由引理 8 即知 -1 为 K 中四平方和，即 $s(K)\leqslant 4$. 这就完成了定理 2 的证明.

定理 2 的整个证明都是构造性的，即证明过程实际上给出了在虚二次域中将 -1 表成最少个数的平方和的具体办法.

【例 1】 $K=\mathbf{Q}(\sqrt{-7})$. 由定理 3 知 $s(K)=4$. 由于 $7=1^2+1^2+1^2+2^2$，从而 $0=1^2+1^2+1^2+2^2+(\sqrt{-7})^2$. 从而 $-2^2=1^2+1^2+1^2+(\sqrt{-7})^2$，于是

$$-1=\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{\sqrt{-7}}{2}\right)^2.$$

(当然还有许多方法，最简单方法是 $-1=1^2+1^2+2^2+(\sqrt{-7})^2$.)

【例 2】 $K=\mathbf{Q}(\sqrt{-6})$. 由定理 3 知 $s(K)=2$. 由于 6 可表成三整数平方和：$6=1^2+1^2+2^2$. 于是 $-(1^2+1^2)=2^2+(\sqrt{-6})^2$. 从而

$$-1=\frac{2^2+(\sqrt{-6})^2}{1^2+1^2}=\left[1^2+\left(\frac{\sqrt{-6}}{2}\right)^2\right](1^2+1^2)$$

$$=\left(1\cdot 1-\frac{\sqrt{-6}}{2}\cdot 1\right)^2+\left(1\cdot 1+1\cdot\frac{\sqrt{-6}}{2}\right)^2$$

$$=\left(\frac{2-\sqrt{-6}}{2}\right)^2+\left(\frac{2+\sqrt{-6}}{2}\right)^2.$$

4. $s(F)=2^n$（费斯特定理）

我们在上小节证明了，对于虚二次域 K，$s(K)$ 只取 1, 2 或 4. 事实上，运用代数数论的进一步知识，可以证明，对于任意代数数域 K，K 中每个全正元均是 K 中四平方和. 特别当 K 不是有序域时，则 -1 是四平方和. 于是 $s(K)\leqslant 4$. 再由

引理 9 便知对于不是有序域的每个代数数域 K，$s(K)$ 均只取三个可能的值：1，2 和 4．显然 $s(K)=1\Leftrightarrow\sqrt{-1}\in K$．而何时 $s(K)=2$ 或 $s(K)=4$，在一般情形下需要用更多的代数数论知识才能说清楚．

1932 年，德国数学家范·德·瓦尔登(van der Waerden)提出这样的问题：哪些整数可以是某个域 F 的 $s(F)$ 值？1966 年，德国人费斯特彻底解决了这个问题．他证明了：

费斯特定理 (1) 对于每个没有序的域 F，$s(F)$ 只能取值为 $2^n(n\geqslant 0)$．(2) 对于每个非负整数 n，均存在域 F，使得 $s(F)=2^n$．

我们在这一小节里证明费斯特定理的第(1)部分．因为它的证明是非常初等的．至于第(2)部分的证明，即对每个 $n\geqslant 0$ 我们构作一个域 F，使得 $s(F)=2^n$，则留到下一小节去证明．

我们以 $G_n(F)$ 表示域 F 中可表成 n 平方和的那些非零元素全体，即

$$G_n(F)=\{\alpha\in F\,|\,\alpha=\beta_1^2+\cdots+\beta_n^2\neq 0,\ \beta_i\in F\}.$$

让我们再看一下引理 9 的证明后面的注记，便会发现我们在证明 $s(F)\neq 3$ 时，关键是利用了"两个二平方和之积仍是二平方和"这一事实，即 $G_2(F)\cdot G_2(F)\subseteq G_2(F)$．由于我们还知道"两个四平方和之积仍是四平方和"，即 $G_4(F)\cdot G_4(F)\subseteq G_4(F)$，由此可以完全类似地证明 $s(F)$ 不能取值 5、6 和 7．证明是非常简单的：如果 -1 在域 F 中是七平方和，即 $-1=a_1^2+\cdots+a_7^2$，其中 $a_i\in F$，则

$$-(1+a_1^2+a_2^2+a_3^2)=a_4^2+a_5^2+a_6^2+a_7^2.$$

如果 $1+a_1^2+a_2^2+a_3^2=0$，则 $-1=a_1^2+a_2^2+a_3^2$，于是 $s(F)\leqslant 3$．如果 $1+a_1^2+a_2^2+a_3^2\neq 0$，则

$$-1=\frac{a_4^2+a_5^2+a_6^2+a_7^2}{1+a_1^2+a_2^2+a_3^2}$$
$$=\left[\left(\frac{a_4}{d}\right)^2+\left(\frac{a_5}{d}\right)^2+\left(\frac{a_6}{d}\right)^2+\left(\frac{a_7}{d}\right)^2\right]$$
$$\cdot(1+a_1^2+a_2^2+a_3^2).$$

其中 $d=1+a_1^2+a_2^2+a_3^2\neq 0$. 但是右边为两个四平方和之积，从而仍为四平方和. 因此 -1 可表成四平方和，即 $s(F)\leqslant 4$. 总之，我们证明了：若 $s(F)\leqslant 7$，则 $s(F)\leqslant 4$. 这就表明 $s(F)$ 不能取值 5, 6, 7. (注意 $s(F)\leqslant 5\Rightarrow s(F)\leqslant 6\Rightarrow s(F)\leqslant 7\Rightarrow s(F)\leqslant 4$.)

为了证明费斯特定理的(1)，自然会想到：是否对每个域 F 和每个 $n\geqslant 0$，均有 $G_{2^n}(F)G_{2^n}(F)\subseteq G_{2^n}(F)$？即是否 F 中两个 2^n 平方和之积仍是 2^n 平方和？答案是肯定的. 我们首先证明：

引理 10 设 F 为域，$n\geqslant 0$，$m=2^n$，$c=c_1^2+\cdots+c_m^2$，$c_i\in F$. 定义

$$\delta_{ij}=\begin{cases}1, & \text{如果 } i=j;\\ 0, & \text{如果 } i\neq j\end{cases}\quad(1\leqslant i\leqslant m,\ 1\leqslant j\leqslant m).$$

则域 F 中存在 m^2 个元素 $\{s_{ij}|1\leqslant i,\ j\leqslant m\}$，满足下列条件：

(1) $s_{1j}=c_j\quad(1\leqslant j\leqslant m)$;

(2) $\sum\limits_{k=1}^{m}s_{ik}s_{jk}=\sum\limits_{k=1}^{m}s_{ki}s_{kj}=\delta_{ij}c\quad(1\leqslant i\leqslant m,\ 1\leqslant j\leqslant m)$.

证明 若 $n=0$，则 $m=1$，$c=c_1^2$. 取 $s_{11}=c_1$ 即可. 现在我们对 n 作数学归纳. 设 $n\geqslant 1$，并且引理对 $n-1$ 的情形成立.

(i) 先设 $c=0$. 如果所有 c_i 均为零，则所有 s_{ij} 均取零值即可. 现设 c_i 不全为零，不妨设 $c_1\neq 0$(否则，适当调整 c_i 的下标和 s_{ij} 的第一个下标即可)，令 $s_{ij}=c_ic_j/c_1$，则 $s_{1j}=c_j(1\leqslant j\leqslant m)$，并且

$$\sum_k s_{ik}s_{jk}=c_1^{-2}\sum_k c_ic_kc_jc_k=c_1^{-2}c_ic_j\sum_k c_k^2=c_1^{-2}c_ic_jc=0.$$

同样地，$\sum_k s_{ki}s_{kj}=0$. 从而如此选取的 s_{ij} 满足引理中两个条件.

(ii) 设 $c\neq0$. 令 $a=c_1^2+\cdots+c_{2^{n-1}}^2$, $b=c_{2^{n-1}+1}^2+\cdots+c_{2^n}^2$. 由于 $c=a+b\neq0$, 从而 a 和 b 不全为零. 不妨设 $a\neq0$（当 $b\neq0$ 时可类似证明）. 由归纳假设可知存在 F 中元素 $\{a_{ij}, b_{ij}|1\leqslant i\leqslant2^{n-1}, 1\leqslant j\leqslant2^{n-1}\}$，使得

i) $a_{1j}=c_j$, $b_{1j}=c_{2^{n-1}+j}(1\leqslant j\leqslant2^{n-1})$.

ii) $\sum_{k=1}^{2^{n-1}}a_{ik}a_{jk}=\sum_{k=1}^{2^{n-1}}a_{ki}a_{kj}=a\delta_{ij}\quad(1\leqslant i,\ j\leqslant2^{n-1})$,

$\sum_{k=1}^{2^{n-1}}b_{ik}b_{jk}=\sum_{k=1}^{2^{n-1}}b_{ki}b_{kj}=b\delta_{ij}\quad(1\leqslant i,\ j\leqslant2^{n-1})$.

现在我们对于 $1\leqslant i,\ j\leqslant2^{n-1}$，令

$$s_{ij}=a_{ij},\ s_{i,2^{n-1}+j}=b_{ij},\ s_{2^{n-1}+i,2^{n-1}+j}=a_{ji},$$

$$s_{2^{n-1}+i,j}=-a^{-1}\sum_{t,l=1}^{2^{n-1}}a_{ti}b_{lt}a_{lj}.$$

显然 $s_{1j}=a_{1j}=c_j$, $s_{1,2^{n-1}+j}=b_{1j}=c_{2^{n-1}+j}(1\leqslant j\leqslant2^{n-1})$, 从而引理中条件(1)成立. 另一方面，对于 $1\leqslant i,\ j\leqslant2^{n-1}$，由 i) 和 ii) 可知

$$\sum_{k=1}^{m}s_{ik}s_{jk}=\sum_{k=1}^{2^{n-1}}a_{ik}a_{jk}+\sum_{k=1}^{2^{n-1}}b_{ik}b_{jk}=(a+b)\delta_{ij}=c\delta_{ij}.$$

$$\sum_{k=1}^{m}s_{ki}s_{kj}=\sum_{k=1}^{2^{n-1}}a_{ik}a_{jk}+a^{-2}\sum_{k=1}^{2^{n-1}}\Big(\sum_{t,l}a_{tk}b_{lt}a_{li}\Big)\Big(\sum_{t',l'}a_{t'k}b_{l't'}a_{l'j}\Big)$$

$$=a\delta_{ij}+a^{-2}\sum_{t,l,t',l'}b_{lt}a_{li}b_{l't'}a_{l'j}\sum_k a_{tk}a_{t'k}$$

$$=a\delta_{ij}+a^{-1}\sum_{t,l,t',l'}b_{lt}a_{li}b_{l't'}a_{l'j}\delta_{tt'}$$

$$=a\delta_{ij}+a^{-1}\sum_{t,l,l'}b_{lt}a_{li}b_{l't}a_{l'j}\quad（根据\ \delta_{tt'}\ 定义）$$

$$=a\delta_{ij}+a^{-1}\sum_{l,l'}a_{li}a_{l'j}\sum_t b_{lt}b_{l't}$$

$$=a\delta_{ij}+a^{-1}b\sum_{l,l'}a_{li}a_{l'j}\delta_{ll'}$$

$$=a\delta_{ij}+a^{-1}b\sum_l a_{li}a_{lj}=a\delta_{ij}+b\delta_{ij}=c\delta_{ij}.$$

$$\sum_{k=1}^{m}s_{2^{n-1}+i,k}s_{jk}=\sum_{k=1}^{2^{n-1}}(-a^{-1})\sum_{t,l}a_{ti}b_{lt}a_{lk}a_{jk}+\sum_{k=1}^{2^{n-1}}a_{ki}b_{jk}$$

$$=(-a^{-1})\sum_{t,l}a_{ti}b_{lt}\sum_k a_{lk}a_{jk}+\sum_k a_{ki}b_{jk}$$

$$=-\sum_{t,l}a_{ti}b_{lt}\delta_{lj}+\sum_k a_{ki}b_{jk}$$

$$=-\sum_t a_{ti}b_{jt}+\sum_k a_{ki}b_{jk}=0=c\delta_{2^{n-1}+i,j}.$$

$$\sum_{k=1}^{m}s_{k,2^{n-1}+i}s_{kj}=\sum_{k=1}^{2^{n-1}}b_{ki}a_{kj}+\sum_{k=1}^{2^{n-1}}a_{ik}(-a^{-1})\sum_{t,l}a_{tk}b_{lt}a_{lj}$$

$$=0=c\delta_{2^{n-1}+i,j}.$$

同样可证:

$$\sum_{k=1}^{m}s_{2^{n-1}+i,k}s_{2^{n-1}+j,k}=\sum_{k=1}^{m}s_{k,2^{n-1}+i}s_{k,2^{n-1}+j}=c\delta_{ij}.$$

于是$\{s_{ij}|1\leqslant i,\ j\leqslant m\}$即为所求.

注记: 上述计算看不出问题的实质. 如果大家知道矩阵的运算,我们可以把证明叙述得更易理解:我们的引理是要求找到m阶方阵$S=(s_{ij})(1\leqslant i,\ j\leqslant m)$, 使得$S^TS=SS^T=cI_m$ (其中S^T表示方阵S的转置, I_m为m阶单位方阵),并且要求$c_1,\cdots,c_m$是S的第一行. 像引理证明那样取$2^{n-1}=\frac{m}{2}$阶方阵$A=(a_{ij})$和$B=(b_{ij})$,使得$A^TA=AA^T=aI_{2^{n-1}}$, $B^TB=BB^T=bI_{2^{n-1}}$, 并且A的第一行为$(c_1,\cdots,c_{2^{n-1}})$, B的第一行为$(c_{2^{n-1}+1},\cdots,c_m)$(由归纳假设保证$A$, B的存在性). 则我们在引理中所构作的方阵S实际上是

$$S=\begin{pmatrix} A & B \\ -a^{-1}A^TB^TA & A^T \end{pmatrix}.$$

利用矩阵运算容易验证 $S^TS=SS^T=cI_m$，并且 S 的第一行为 $(c_1, \cdots, c_m)$.

现在我们证明：

定理 3 设 F 为域，$n\geqslant 0$, $m=2^n$，则

$$G_m(F)\cdot G_m(F)=G_m(F).$$

换句话说：域 F 中两个 m 平方和之乘积仍是 m 平方和.

证明 设 $u_1, \cdots, u_m, v_1, \cdots, v_m\in F$. 由引理 10 可知存在 F 中元素 $\{s_{ij}|1\leqslant i, j\leqslant m\}$ 和 $\{t_{ij}|1\leqslant i, j\leqslant m\}$. 使得

$$s_{1j}=u_j,\ t_{1j}=v_j \quad (1\leqslant j\leqslant m),$$

$$\sum_k s_{ik}s_{jk}=\sum_k s_{ki}s_{kj}=u\delta_{ij},$$

$$\sum_k t_{ik}t_{jk}=\sum_k t_{ki}t_{kj}=v\delta_{ij},$$

其中 $u=u_1^2+\cdots+u_m^2$, $v=v_1^2+\cdots+v_m^2$. 现在令

$$w_i=\sum_{k=1}^m v_{1k}u_{ik} \quad (1\leqslant i\leqslant m),$$

则

$$\begin{aligned} w_1^2+w_2^2+\cdots+w_m^2 &= \sum_{l=1}^m\left(\sum_{k=1}^m v_{1k}u_{lk}\right)\left(\sum_{k'=1}^m v_{1k'}u_{lk'}\right) \\ &= \sum_{k,k'} v_{1k}v_{1k'}\sum_l u_{lk}u_{lk'} \\ &= \sum_{k,k'} v_{1k}v_{1k'}u\delta_{kk'} \\ &= u\sum_k v_{1k}v_{1k}=uv\delta_{11}=uv \\ &= (u_1^2+\cdots+u_m^2)(v_1^2+\cdots+v_m^2). \end{aligned}$$

这就表明 F 中两个 m 平方和之乘积仍是 m 平方和，从而 $G_m(F)G_m(F)\subseteq G_m(F)$. 另一方面，$G_m(F)=G_m(F)\cdot 1\subseteq G_m(F)G_m(F)$. 于是 $G_m(F)G_m(F)=G_m(F)$. 证毕.

现在我们证明费斯特定理的第(1)部分，即对于任意域 F，$s(F)$ 只取形如 2^n 的值。我们只需证明：若 $2^{n-1}<m<2^n$，而 $s(F)\leqslant m$，则必然 $s(F)\leqslant 2^{n-1}$。因为这就表明 $s(F)$ 不能取 2 的方幂以外的值。由假定知，存在 $a_1, \cdots, a_m\in F$，使得 $-1=a_1^2+\cdots+a_m^2$，注意 $m>2^{n-1}$，从而又可写为 $-(1+a_1^2+\cdots+a_{m-2^{n-1}}^2)=a_{m-2^{n-1}+1}^2+\cdots+a_m^2$。此式右边为 2^{n-1} 平方和，而左边括号内平方项数为 $1+m-2^{n-1}\leqslant 2^n-1+1-2^{n-1}=2^{n-1}$。于是可加上一些 0^2 使得左边括号内也是 2^{n-1} 平方和。从而我们有公式

$$-(u_1^2+\cdots+u_{2^{n-1}}^2)=v_1^2+\cdots+v_{2^{n-1}}^2.$$

即

$$-1=\frac{(u_1^2+\cdots+u_{2^{n-1}}^2)(v_1^2+\cdots+v_{2^{n-1}}^2)}{(u_1^2+\cdots+u_{2^{n-1}}^2)^2}\in G_{2^{n-1}}(F)G_{2^{n-1}}(F)$$
$$=G_{2^{n-1}}(F).$$

于是 $s(F)\leqslant 2^{n-1}$。证毕。

四、多项式平方和

1. 历史的回顾

前两节我们谈的是整数平方和，第三节我们逐渐谈到任意域上的平方和问题. 我们讲述了阿廷-施莱尔结果：域 F 中元素 a 是 F 中平方和的充要条件是 a 为 F 中的全正元素. 本节中我们又回到一个具体的域，即实数域 $\mathbf{R}$ 上的多变量有理函数域 $\mathbf{R}(x_1, \cdots, x_n)$. 我们要研究这个域上的平方和问题.

用 $\mathbf{R}[x_1, x_2, \cdots, x_n]$ 表示以 $x_1, \cdots, x_n$ 为未定元的实系数多项式全体. 大家知道两个实系数多项式 $f(x_1, \cdots, x_n)$ 和 $g(x_1, \cdots, x_n)$ 是如何相加、减和相乘的，并且所得结果仍是实系数多项式. 于是 $\mathbf{R}[x_1, \cdots, x_n]$ 是环，叫作 $\mathbf{R}$ 上对于 $x_1, \cdots, x_n$ 的多项式环. 两个这样的多项式相除(即写成分式，其中分母不为零)叫作 $\mathbf{R}$ 上关于 $x_1, \cdots, x_n$ 的有理函数. 有理函数之间可以作四则运算. 所以形成域，叫作 $\mathbf{R}$ 上关于 $x_1, \cdots, x_n$ 的有理函数域，表示成 $\mathbf{R}(x_1, \cdots, x_n)$. 我们今后将看到这是有序域，从而 -1 在 $\mathbf{R}(x_1, \cdots, x_n)$ 中不是平方和. 而有理函数 $\alpha=\alpha(x_1, \cdots, x_n)\neq 0$ 为平方和的充要条件是 α 为全正元素，即对于 $\mathbf{R}(x_1, \cdots, x_n)$ 的每个序，α 均是正元素. 但为了判别 α 是否为全正元，需要知道域 $\mathbf{R}(x_1, \cdots, x_n)$ 的所有可能的序，这是不容易的. 但是可以考虑比较容易的事情：

如果有理函数 $\alpha=\alpha(x_1, \cdots, x_n)$ 可以表成平方和，即存在多项式 $f_i(x_1, \cdots, x_n)$, $g_i(x_1, \cdots, x_n)\in \mathbf{R}[x_1, \cdots, x_n](1\leqslant i\leqslant m)$，使得

$$\alpha(x_1, \cdots, x_n)=\left(\frac{f_1(x_1, \cdots, x_n)}{g_1(x_1, \cdots, x_n)}\right)^2+\cdots+\left(\frac{f_m(x_1, \cdots, x_n)}{g_m(x_1, \cdots, x_n)}\right)^2.$$

那么将 $x_1, \cdots, x_n$ 代入任意一组实数 $(a_1, \cdots, a_n)$，只要上式两边有意义(即分母取值不为零)，必然

$$\alpha(a_1, \cdots, a_n)=\left(\frac{f_1(a_1, \cdots, a_n)}{g_1(a_1, \cdots, a_n)}\right)^2+\cdots+\left(\frac{f_m(a_1, \cdots, a_n)}{g_m(a_1, \cdots, a_n)}\right)^2\geqslant 0.$$

具有这样性质的有理函数 α 叫作正定的．换句话说，我们有如下的定义：

定义 实系数有理函数 $\alpha(x_1, \cdots, x_n)$ 叫做正定的，是指对任意实数 $a_1, \cdots, a_n$，只要 $\alpha(a_1, \cdots, a_n)$ 有意义(即分母不为零)，则必然 $\alpha(a_1, \cdots, a_n)\geqslant 0$.

由上述可知，域 $\mathbf{R}(x_1, \cdots, x_n)$ 中每个平方和必然是正定的．反过来对吗？1900 年，希尔伯特著名的二十三个问题中，便有一个是：

希尔伯特第十七问题 关于 $x_1, \cdots, x_n$ 的实系数正定有理函数是否一定可表成有限个关于 $x_1, \cdots, x_n$ 的实系数有理函数的平方和？

如果答案是肯定的，那么我们实质上是对于域 $\mathbf{R}(x_1, \cdots, x_n)$ 中全正元素给出了另一种刻划方式．因为若答案是肯定的，则便有：

$$\alpha=\alpha(x_1, \cdots, x_n)\text{正定}\Leftrightarrow\alpha\text{是平方和}\Leftrightarrow\alpha\text{全正}.$$

正是为了攻克这个问题，阿廷和施莱尔于1926年建立了形式实域理论，他们发现形式实域和有序域这两个概念是等价的. 然后又证明了"α为域F中平方和"和"α为F中全正元素"等价. 阿廷将他们发展的理论用于域$\mathbf{R}(x_1, \cdots, x_n)$，证明了全正元素和正定元素这两个概念是一致的，从而肯定地解决了希尔伯特第十七问题.

阿廷的证明和后人给出的其他证明方法都需要较多的数学知识，在本书中就不作介绍了. 我们想谈的是下面的问题：$\mathbf{R}[x_1, \cdots, x_n]$中每个正定多项式是否一定可表成$\mathbf{R}[x_1, \cdots, x_n]$中有限个多项式的平方和？（根据阿廷的结果，它一定是$\mathbf{R}(x_1, \cdots, x_n)$中有限个有理函数的平方和.）希尔伯特早在1888年就研究了这个问题. 为了介绍希尔伯特的结果，我们需要两个简单的引理.

引理1 设$f(x_1, \cdots, x_n)$是实系数非零多项式，则必存在n个实数$a_1, \cdots, a_n$，使得$f(a_1, \cdots, a_n)\neq 0$. 换句话说，如果对任意实数$a_1, \cdots, a_n$，$f(a_1, \cdots, a_n)$均为零，则多项式$f$恒为零.

证明 我们对多项式f的变量个数n作数学归纳. 当$n=0$时，f为常数a. 由假设知$a\neq 0$，于是引理1显然成立. 当$n=1$时，$f=f(x)$是非零多项式. 它的实根只有有限个（其个数不超过f的次数）. 因此存在实数a_1，使得$f(a_1)\neq 0$. 现设引理对$n-1$成立，令$n\geqslant 2$. 如果$f(x_1, \cdots, x_n)$中不出现x_n，则化为$n-1$的情形，由归纳假设知引理1成立. 现设f中出现x_n，于是将f按x_n展开：

$$f=x_n^d g_d(x_1, \cdots, x_{n-1})+x_n^{d-1}g_{d-1}(x_1, \cdots, x_{n-1})+\cdots$$
$$+x_n g_1(x_1, \cdots, x_{n-1})+g_0(x_1, \cdots, x_{n-1}).$$

其中$d\geqslant 1$，$g_d(x_1, \cdots, x_{n-1})$不恒为零. 由归纳假设，存在实

数 $a_1, \cdots, a_{n-1}$，使得 $g_d(a_1, \cdots, a_{n-1}) \neq 0$. 令 $c_i = g_i(a_1, \cdots, a_{n-1})$，则 $f(a_1, \cdots, a_{n-1}, a_n) = c_d x_n^d + c_{d-1} x_n^{d-1} + \cdots + c_1 x_n + c_0$，其中 $c_i \in \mathbf{R}$，$c_d \neq 0$. 于是这个多项式至多有 d 个实根，从而存在实数 a_n，使得 $f(a_1, \cdots, a_{n-1}, a_n) \neq 0$. 证毕.

注记：上面证明只用到实数域具有无限多个元素. 所以将实数域改成任何无限域，引理 1 均成立. 另一方面，引理 1 对于有限域不再成立. 如对于二元域 $F = \{0, 1\}$（其中 $1+1=0$），多项式 $x^2 - x$ 不恒为零，但是 F 中所有元素均是它的根.

设 $f(x_1, \cdots, x_n)$ 是实系数多项式（或者系数属于任意域 F），f 的每个单项式有形式 $ax_1^{r_1}x_2^{r_2}\cdots x_n^{r_n}$，其中 a 为非零实数（或域 F 中非零元素），我们称这个单项式的次数为 $r_1 + r_2 + \cdots + r_n$，而它对于变量 x_i 的次数为 $r_i (1 \leqslant i \leqslant n)$. 多项式 f 中包含的单项式次数的最大值叫作 f 的次数. 同样地 f 包含的所有单项式对 x_i 次数的最大值叫作 f 对 x_i 的次数. 例如 $f(x_1, x_2, x_3) = x_1x_2x_3 + x_1^2$ 的次数为 3，而对于 x_1，x_2 和 x_3 的次数分别为 2，1 和 1. 若 f 中每个单项式的次数均为 m，则 f 叫做 m 次齐次多项式. m 次实系数多项式 $f(x_1, \cdots, x_n)$ 按单项式展开可写成

$$f(x_1, \cdots, x_n) = \sum_{\substack{i_1, \cdots, i_n \geqslant 0 \\ i_1 + \cdots + i_n \leqslant m}} a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}.$$

由于 f 的次数为 m，从而必有某组 $i_1, \cdots, i_n$，$i_1 + \cdots + i_n = m$，使得 $a_{i_1 \cdots i_n} \neq 0$. 而多项式

$$\begin{aligned} F(x_0, x_1, \cdots, x_n) &= x_0^m f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}, \cdots, \frac{x_n}{x_0}\right) \\ &= \sum_{\substack{i_1, \cdots, i_n \geqslant 0 \\ i_1 + \cdots + i_n \leqslant m}} x_0^m x_1^{i_1} \cdots x_n^{i_n} x_0^{-i_1 - i_2 - \cdots - i_n} \end{aligned}$$

$$= \sum_{\substack{i_0, i_1, \cdots, i_n \geq 0 \\ i_0+i_1+\cdots+i_n=m}} a_{i_1 \cdots i_n} x_0^{i_0} x_1^{i_1} \cdots x_n^{i_n} \quad (i_0 = m - i_1 - \cdots - i_n)$$

是关于 x_0, x_1, …, x_n 的 m 次齐次多项式. 注意 $F(1, x_1, \cdots, x_n) = f(x_1, \cdots, x_n)$. 而对 m 次齐次多项式 $F(x_0, x_1, \cdots, x_n)$, 则 $F(\alpha x_0, \alpha x_1, \cdots, \alpha x_n) = \alpha^m F(x_0, \cdots, x_n)$, 其中 α 为任意实数.

引理 2 设 $f(x_1, \cdots, x_n)$ 为 m 次实系数多项式, f 不恒为零, 则 f 为正定的 $\Leftrightarrow$ 齐次多项式

$$F(x_0, \cdots, x_n) = x_0^m f\left(\frac{x_1}{x_0}, \cdots, \frac{x_n}{x_0}\right)$$

为正定的.

证明 若 $m=0$, 则 $f=F=a\in \mathbf{R}$. 而 f 正定 $\Leftrightarrow a\geqslant 0 \Leftrightarrow F$ 正定, 从而引理显然成立. 下设 $m\geqslant 1$. 若 $F(x_0, \cdots, x_n)$ 正定, 则 $f(x_1, \cdots, x_n) = F(1, x_1, \cdots, x_n)$ 正定. 反之, 若 $f(x_1, \cdots, x_n)$ 正定, 则 $f(x_1, \cdots, x_n) = f_m(x_1, \cdots, x_n) + f_{m-1}(x_1, \cdots, x_n) + \cdots + f_1(x_1, \cdots, x_n) + f_0(x_1, \cdots, x_n)$, 其中 $f_i(x_1, \cdots, x_n)$ 是 f 的所有 i 次单项式之和. 当 $f_i \neq 0$ 时, f_i 是 i 次齐次多项式. 于是对每个实数 λ,

$$\begin{aligned} f(\lambda x_1, \cdots, \lambda x_n) = & \lambda^m f_m(x_1, \cdots, x_n) \\ & + \lambda^{m-1} f_{m-1}(x_1, \cdots, x_n) + \cdots \\ & + f_0(x_1, \cdots, x_n). \end{aligned} \quad ①$$

由于 f 的次数为 m, 从而 $f_m \neq 0$. 于是存在实数 $a_1, \cdots, a_n$, 使得 $f_m(a_1, \cdots, a_n) \neq 0$(引理 1). 由 ① 式知当 λ 的绝对值很大时, $f(\lambda a_1, \cdots, \lambda a_n)$ 的符号与 $\lambda^m f(a_1, \cdots, a_n)$ 的符号一致, 因为 ① 式右边第一项的值起主要作用. 如果 m 为奇数, 则当 λ 绝对值很大时 $\lambda^m f_m(a_1, \cdots, a_n)$ 和 $(-\lambda)^m f_m(a_1, \cdots, a_n) = -\lambda^m f_m(a_1, \cdots, a_n)$ 符号相反, 因此 $f(\lambda a_1, \cdots, \lambda a_n)$ 和 $f(-\lambda a_1,$

$\cdots, -\lambda a_n)$一正一负，这与 f 正定矛盾. 因此 m 必为偶数，并且 $f_m(a_1, \cdots, a_n) > 0$. 从而 $f_m(x_1, \cdots, x_n)$ 必然是正定的. 由于

$$
\begin{aligned}
& F(x_0, x_1, \cdots, x_n) \\
& \quad = x_0^m f\left(\frac{x_1}{x_0}, \cdots, \frac{x_n}{x_0}\right) = x_0^m (x_0^{-m} f_m(x_1, \cdots, x_n) \\
& \qquad + x_0^{-(m-1)} f_{m-1}(x_1, \cdots, x_n) + \cdots + f_0(x_1, \cdots, x_n)) \\
& \quad = f_m(x_1, \cdots, x_n) + x_0 f_{m-1}(x_1, \cdots, x_n) \\
& \qquad + x_0^m f_0(x_1, \cdots, x_n),
\end{aligned}
$$

因此对任意实数 $a_1, \cdots, a_n$, $F(0, a_1, \cdots, a_n) = f_m(a_1, \cdots, a_n) \geqslant 0$. 而当 a_0 为非零实数时, $F(a_0, a_1, \cdots, a_n) = a_0^m f\left(\frac{a_1}{a_0}, \cdots, \frac{a_n}{a_0}\right) \geqslant 0$. (由于 m 为偶数而 f 正定.) 这就证明 F 正定. 证毕.

引理 3 设 $f(x_1, \cdots, x_n)$ 为 m 次实系数多项式, $m \geqslant 1$. 则 $f(x_1, \cdots, x_n)$ 为实系数多项式平方和 $\Leftrightarrow F(x_0, \cdots, x_n) = x_0^m f\left(\frac{x_1}{x_0}, \cdots, \frac{x_n}{x_0}\right)$ 为实系数多项式平方和.

证明 如果 f 是实系数多项式平方和, 即

$$
f(x_1, \cdots, x_n) = f_1(x_1, \cdots, x_n)^2 + \cdots + f_d(x_1, \cdots, x_n)^2, \quad ②
$$

其中 $f_1, \cdots, f_d$ 均是实系数多项式. 则 f 正定, 从而 m 为偶数 (见引理 2 的证明). 令 $m = 2s$, 则

$$
\begin{aligned}
F(x_0, \cdots, x_n) &= x_0^{2s} f\left(\frac{x_1}{x_0}, \cdots, \frac{x_n}{x_0}\right) \\
&= \left[x_0^s f_1\left(\frac{x_1}{x_0}, \cdots, \frac{x_n}{x_0}\right)\right]^2 + \cdots \\
&\quad + \left[x_0^s f_d\left(\frac{x_1}{x_0}, \cdots, \frac{x_n}{x_0}\right)\right]^2. \qquad ③
\end{aligned}
$$

设 $f_1, \cdots, f_d$ 的次数最大值为 l. 如果 $l>s$, 不妨设 $f_1, \cdots, f_r$ 的次数为 l, $f_{r+1}, \cdots, f_d$ 的次数小于 l, 其中 $r\geqslant 1$. 令 $g_i(x_1, \cdots, x_n)$ 为 $f_i(x_1, \cdots, x_n)$ 中所有 l 次单项式之和 $(1\leqslant i\leqslant r)$. 将 ② 式右边展开, 它的最高次数为 $2l$, 而 $2l$ 次部分为 $g_1^2+\cdots+g_r^2$. 但是 ② 式左边次数为 $2s<2l$, 即左边没有 $2l$ 次部分. 于是

$$0=g_1^2+\cdots+g_r^2 \quad (r\geqslant 1). \qquad ④$$

由于 $g_1(x_1, \cdots, x_n)\neq 0$, 从而有实数 $a_1, \cdots, a_n$, 使得 $g_1(a_1, \cdots, a_n)\neq 0$(引理 1). 于是 $g_1(a_1, \cdots, a_n)^2+\cdots+g_r(a_1, \cdots, a_n)^2>0$, 而这与 ④ 式矛盾. 这表明 $l\leqslant s$, 即 $f_1, \cdots, f_d$ 的次数均不超过 s. 从而 ③ 式右边是关于 $x_0, \cdots, x_n$ 的 d 个多项式的平方和. 这就证明了若 f 为多项式平方和, 则齐次多项式 $F(x_0, \cdots, x_n)$ 也是多项式平方和. 反之, 若 $F(x_0, \cdots, x_n)$ 为多项式平方和, 即

$$F(x_0, x_1, \cdots, x_n)=F_1(x_0, x_1, \cdots, x_n)^2+\cdots +F_d(x_0, \cdots, x_n)^2,$$

则 $f(x_1, \cdots, x_n)=F(1, x_1, \cdots, x_n)=F_1(1, x_1, \cdots, x_n)^2+\cdots+F_d(1, x_1, \cdots, x_n)^2$, 即 f 也是多项式平方和. 证毕.

基于引理 2 和引理 3, 为了考查实系数正定多项式是否为实系数多项式平方和, 我们只需考虑实系数正定齐次多项式即可. 对于 $n, m\geqslant 1$, 我们以 $P_{n,2m}$ 表示 n 个变量 $x_1, \cdots, x_n$ 的实系数正定 $2m$ 次齐次多项式全体(由引理 2 的证明可知, 正定齐次多项式的次数必为偶数), 而以 $\Sigma_{n,2m}$ 表示可表成实系数多项式平方和的关于 $x_1, \cdots, x_n$ 的 $2m$ 次齐次多项式全体. 由于可表成多项式平方和的多项式必然正定, 从而 $\Sigma_{n,2m}\subseteq P_{n,2m}$. 希尔伯特于 1888 年证明了:

当 $(n, 2m)=(n, 2)$ (任意 $n\geqslant 1$), $(2, 2m)$ (任意 $m\geqslant 1$)

和(3, 4)时 $\Sigma_{n,2m}=P_{n,2m}$. 而对于$(n, 2m)$的其他值, $\Sigma_{n,2m}\neq P_{n,2m}$. 即对于$(n, 2m)$的其他值，均存在 n 个变量 $x_1, \cdots, x_n$ 的实系数 $2m$ 次正定齐次多项式不为实系数多项式平方和.

希尔伯特的证明是用复杂的代数几何方法，证明是非构造性的，即并没有给出不能表成实系数多项式平方和的正定齐次多项式的具体例子. 而第一个这样的具体例子是八十年后由 Motzkin 于 1967 年给出的. 他证明了

$$M(x_1, x_2, x_3)=x_1^6+x_2^4x_3^2+x_2^2x_3^4-3x_1^2x_2^2x_3^2$$

是正定的，但不能表成实系数多项式平方和. 即 $M(x_1, x_2, x_3)\in P_{3,6}-\Sigma_{3,6}$. Robinson 于 1973 年又给出这样的一些例子. 例如他证明了对每个 $n\geqslant 1$,

$$F(x_0, \cdots, x_n)=x_1^2\cdots x_n^2(x_1^2+\cdots+x_n^2-(n+1)x_0^2)+x_0^{2n+2}$$
$$\in P_{n+1,2n+2}-\Sigma_{n+1,2n+2}.$$

当 $n=2$ 时，这就是 $M(x_1, x_2, x_3)$.（很容易证明 F 是正定的. 只需用"算术平均值≥几何平均值"公式，留给读者练习.）1975 年，蔡文端证明了

$$x_1^2y_1^2+x_2^2y_2^2+x_3^2y_3^2-2(x_1x_2y_1y_2+x_2x_3y_2y_3+x_3x_1y_3y_1)$$
$$+2(x_1^2y_2^2+x_2^2y_3^2+x_3^2y_1^2)\in P_{4,6}-\Sigma_{4,6}.$$

1977 年，林节玄和蔡文端又给出许多这样的例子，例如证明了

$$w^4+x^2y^2+y^2z^2+z^2x^2-4xyzw\in P_{4,4}-\Sigma_{4,4}.$$
$$x^4y^2+y^4z^2+z^4x^2-3x^2y^2z^2\in P_{3,6}-\Sigma_{3,6}.$$

1978 年，Reznick 给出了许多 $n=3$ 的这样的例子. 本书作者于 1982 年仔细分析了 Reznick 的例子，证明了对每个 $2m\geqslant 6$, 都提供出 $P_{3,2m}-\Sigma_{3,2m}$ 中的例子. 我们在本节第 2 小节证明当 $(n, 2m)=(2, 2m)$ 和 $(n, 2)$ 时, $\Sigma_{n,2m}=P_{n,2m}$, 而在第 3 小节证明上面所举的某些例子确实属于 $P_{n,2m}-\Sigma_{n,2m}$.

我们在第 4 小节要证明第 3.4 小节费斯特定理的第 (2) 部分. 我们令 $s(F)$ 为 -1 在无序域 F 中可表成平方和所需最少元素个数. 我们已经证明了费斯特定理的第(1)部分，即 $s(F)$ 只能等于 2 的方幂. 我们将在第 4 小节利用有理函数域证明对每个 $n\geqslant 0$，均存在无序域 F，使得 $s(F)=2^n$.

最后我们在第 4 小节要介绍关于有理函数域中平方和的另一些有趣结果，并提出一些关于平方和的至今未解决的问题.

练习　设 $F(x_1, \cdots, x_n)$ 是实系数齐次多项式. 如果 F 是实系数多项式的平方和，求证 F 也必是一些实系数齐次多项式的平方和.

2. 多项式平方和——肯定性和否定性结果

采用上小节记号，我们用 $P_{n,2m}$ 表示以 $x_1, \cdots, x_n$ 为变量的实系数正定 $2m$ 次齐次多项式全体. 以 $\Sigma_{n,2m}$ 表示 $P_{n,2m}$ 中可表成实系数多项式平方和的多项式全体. 我们在本小节中要证明当 $(n, 2m)=(2, 2m)$ (m 为任意正整数) 和 $(n, 2)$ (n 为任意正整数)时，$P_{n,2m}=\Sigma_{n,2m}$ (对每个任意正整数 m，显然 $\Sigma_{1,2m}=P_{1,2m}$). 先谈 $n=2$ 的情形.

定理 1　每个实系数 $2m$ 次正定齐次多项式 $F(x, y)\in \mathbf{R}[x, y]$ 均可表成两个实系数多项式的平方和.

证明　设

$$F(x, y)=a_0x^{2m}+a_1x^{2m-1}y+\cdots+a_{2m-1}xy^{2m-1}+a_{2m}y^{2m},$$

由引理 2 即知 $f(x)=F(x, 1)=a_0x^{2m}+a_1x^{2m-1}+\cdots+a_{2m}$ 正定，$f(x)$ 的次数 $\leqslant 2m$. 由于 $f(x)$ 正定，从而 $f(x)$ 的次数为偶数，并且首项系数为正实数(见引理 2 的证明). 于是令 $f(x)$ 的次数为 $2r$ ($r\leqslant m$)，则

$$f(x)=c_0x^{2r}+c_1x^{2r-1}+\cdots+c_{2r}$$
$$=c_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{2r}). \qquad ⑤$$

其中 $c_0>0$，而 $\alpha_1, \cdots, \alpha_{2r}$ 是 $f(x)$ 的 $2r$ 个根. 我们只需证明 $f(x)$ 可表成两个实系数多项式的平方和. 因这时，由引理 3 即知 $y^{2r}f\left(\frac{x}{y}\right)$ 为两个实系数多项式平方和，从而 $F(x, y)=y^{2m}f\left(\frac{x}{y}\right)=(y^{m-r})^2\cdot y^{2r}f\left(\frac{x}{y}\right)$ 也是如此.

大家知道，若 $a+ib$ 为 $f(x)$ 的根，其中 a, b 为实数并且 $b\neq 0$，则它的共轭 $a-ib$ 也是 $f(x)$ 的根，于是⑤式右边有因子

$$(x-(a+ib))(x-(a-ib))$$
$$=[(x-a)-ib][(x-a)+ib]=(x-a)^2+b^2,$$

这是二平方和. 不妨设 f 的 $2r$ 个根中 $\alpha_1, \cdots, \alpha_{2s}$ 为实根，其余 $2(s-r)$ 个为 $s-r$ 对彼此共轭的复根：$\alpha_j=a_j+ib_j$, $\bar{\alpha}_j=a_j-ib_j(b_j\neq 0)(1\leqslant j\leqslant s-r)$，则

$$f(x)=c_0(x-\alpha_1)\cdots(x-\alpha_{2s})\prod_{j=1}^{s-r}[(x-a_j)^2+b_j^2].$$

实根 $\alpha_1, \cdots, \alpha_{2s}$ 中可能有重根. 设其中恰有 l 个彼此不同的实根：$\beta_1>\beta_2>\cdots>\beta_l$，其中根 β_k 的重数为 $\lambda_k(1\leqslant k\leqslant l)$. 则 $\lambda_1+\cdots+\lambda_l=2s$，并且

$$f(x)=c_0\prod_{k=1}^{l}(x-\beta_k)^{\lambda_k}\prod_{j}[(x-a_j)^2+b_j^2]. \qquad ⑥$$

如果 $\lambda_1, \cdots, \lambda_l$ 中有奇数，不妨设 $\lambda_1, \cdots, \lambda_{t-1}$ 均为偶数而 λ_t 为奇数. 我们取实数 a 使 $\beta_t>a>\beta_{t+1}$（若 $t=l$ 则只需取 $a<\beta_l$ 即可），则由 ⑥ 式知

$$f(a)=c_0\left(\prod_{k=1}^{t-1}(a-\beta_k)^{\lambda_k}\right)(a-\beta_t)^{\lambda_t}\left(\prod_{k=t+1}^{l}(a-\beta_k)^{\lambda_k}\right)$$
$$\times\prod_{j}[(a-a_j)^2+b_j^2].$$

注意 $c_0>0$. 当 $1\leqslant k\leqslant t-1$ 时, λ_k 均为偶数并且 $\alpha\neq\beta_k$, 从而乘积 $\prod_{k=1}^{t-1}>0$. 由于 $\alpha<\beta_t$ 而 λ_t 为奇数, 从而 $(\alpha-\beta_t)^{\lambda_t}<0$. 当 $t+1\leqslant k\leqslant l$ 时 $\alpha>\beta_k$, 从而乘积 $\prod_{k=t+1}^{l}>0$. 最后由于 $b_j\neq0$, 从而 $\prod_j>0$. 于是上式给出 $f(\alpha)<0$, 这与 f 正定相矛盾. 于是 $\lambda_k(1\leqslant k\leqslant l)$ 均为偶数. 从而 $c_0\prod_{k=1}^{l}(x-\beta_k)^{\lambda_k}$ 是实系数多项式的平方. 由恒等式

$$(x_1^2+x_2^2)(y_1^2+y_2^2)$$
$$=(x_1y_1+x_2y_2)^2+(x_1y_2-x_2y_1)^2$$

可知, $\prod_{j=1}^{s-r}[(x-a_j)^2+b_j^2]$ 为两个实系数多项式的平方和. 再由⑥式即知 $f(x)$ 也如此. 这就证明了定理 1.

现在研究 $m=1$ 的情形. 这时, 关于 $x_1, \cdots, x_n$ 的实系数二次齐次多项式就是第一小节中见过的所谓二次型.

定理 2 设 $f(x_1, \cdots, x_n)=\sum_{1\leqslant i\leqslant j\leqslant n}a_{ij}x_ix_j$ 为实系数正定二次型, 其中 a_{ij} 均为实数. 则 f 为 n 个实系数多项式的平方和.

证明 我们对 f 的变量个数 n 作归纳法. 当 $n=1$ 时, $f=a_{11}x_1^2$. 若 f 正定则 $a_{11}\geqslant0$, 于是 $f=(\sqrt{a_{11}}x_1)^2$, 其中 $\sqrt{a_{11}}$ 为实数. 即定理对 $n=1$ 成立. 下设 $n\geqslant2$, 并且假设定理对 $n-1$ 个变量的情形成立. 由 $f(1, 0, \cdots, 0)=a_{11}$ 可知 $a_{11}\geqslant0$. 同样可知 $a_{22}, \cdots, a_{nn}\geqslant0$. 如果 $a_{11}=\cdots=a_{nn}=0$, 则 $f(1, -a_{12}, 0, \cdots, 0)=a_{12}\cdot1\cdot(-a_{12})=-a_{12}^2\geqslant0$. 因此 $a_{12}=0$. 类似可知对每个 $1\leqslant i<j\leqslant n$, 均有 $a_{ij}=0$. 这表明 f 恒为零, 这时定理显然成立, 于是下设 $a_{11}, \cdots, a_{nn}$ 不全为零. 不妨设 $a_{11}\neq0$, 于是 $a_{11}>0$. 并且

$$
\begin{aligned}
f(x_1, \cdots, x_n) &= a_{11}x_1^2 + a_{12}x_1x_2 + \cdots + a_{1n}x_1x_n \\
&\quad + \sum_{2 \le i \le j \le n} a_{ij}x_ix_j \\
&= a_{11}\left(x_1 + \frac{a_{12}}{2a_{11}}x_2 + \cdots + \frac{a_{1n}}{2a_{11}}x_n\right)^2 \\
&\quad + \sum_{2 \le i \le j \le n} a_{ij}x_ix_j \\
&\quad - \left(\frac{a_{12}}{2a_{11}}x_2 + \cdots + \frac{a_{1n}}{2a_{11}}x_n\right)^2 \\
&= a_{11}\left(x_1 + \frac{a_{12}}{2a_{11}}x_2 + \cdots + \frac{a_{1n}}{2a_{11}}x_n\right)^2 \\
&\quad + g(x_2, \cdots, x_n), \qquad ⑦
\end{aligned}
$$

其中 $g(x_2, \cdots, x_n)$为关于 $x_2, \cdots, x_n$ 的二次型. 我们证明 g 也是正定的：如果存在实数 $a_2, \cdots, a_n$，使得 $g(a_2, \cdots, a_n)<0$，令 $a_1=-\left(\frac{a_{12}}{2a_{11}}a_2+\cdots+\frac{a_{1n}}{2a_{11}}a_n\right)$，则由 ⑦ 式知

$$f(a_1, a_2, \cdots, a_n)=g(a_2, \cdots, a_n)<0,$$

这与 f 的正定相矛盾，从而 $g(x_2, \cdots, x_n)$正定. 由归纳假设知 g 可表成 $n-1$ 个实系数多项式的平方和. 再由 ⑦ 式（注意 $a_{11}>0$）即知 f 可表成 n 个实系数多项式的平方和. 证毕.

最后，关于$(n, 2m)=(3, 4)$的情形，希尔伯特于 1888 年证明了 $P_{3,4}=\Sigma_{3,4}$. 换句话说，每个实系数正定三元四次齐次多项式均为实系数多项式平方和. 林节玄和蔡文端于 1977 年给了一个简单的证明. 但是由于用到一些非初等数学，这里就不介绍了.

现在我们介绍一些反例，即举出不能表成实系数多项式平方和的实系数正定齐次多项式的具体例子. 根据上述肯定性结果，可知首先要考虑的情形是$(n, 2m)=(3, 6)$和$(4, 4)$。

【例 1】 (A. Lax 和 P. Lax, 1978) 1971 年国际数学奥

林匹克竞赛有这样一道题：

设 n 为正整数，$x_1, \cdots, x_n$ 为 n 个实变量．定义

$$A_n(x_1, \cdots, x_n)=\sum_{i=1}^{n}\prod_{\substack{j=1\\ j\neq i}}^{n}(x_i-x_j),$$

试问对哪些 n 值，A_n 是正定的？

这个问题的答案是 $n=3$ 和 5．证明是这样的：由于 A_n 是 $n-1$ 次齐次多项式，而正定齐次多项式的次数必为偶数．因此若 A_n 正定，则 n 必为奇数．进而若 n 为奇数并且 $n\geqslant 7$，取 $(x_1, \cdots, x_n)=(0, 0, 0, 1, 2, 2, \cdots, 2)$．请读者计算 $A_n(0, 0, 0, 1, 2, \cdots, 2)=\prod\limits_{\substack{j=1\\ j\neq 4}}^{n}(x_4-x_j)=(-1)^{n-4}=-1$．因此若 A_n 正定，n 只能为 3 或 5．由于

$$\begin{aligned}
&A_3(x_1, x_2, x_3)\\
&\quad=(x_1-x_2)(x_1-x_3)+(x_2-x_1)(x_2-x_3)\\
&\qquad+(x_3-x_1)(x_3-x_2)\\
&\quad=\frac{1}{2}[(x_1-x_2)^2+(x_2-x_3)^2+(x_3-x_1)^2],
\end{aligned}$$

可知 A_3 是正定的，并且是多项式平方和．另一方面，我们来证明 A_5 也是正定的：首先注意，从 A_n 的表达式可知 n 个变量 $x_1, \cdots, x_n$ 的地位是完全平等的．也就是说，将公式 A_n 中 $x_1, \cdots, x_n$ 任意交换次序，则 A_n 的表达式不变．因此我们不妨假定 $x_1\geqslant x_2\geqslant x_3\geqslant x_4\geqslant x_5$，将 A_5 写成

$$\begin{aligned}
A_5=&(x_1-x_2)[(x_1-x_3)(x_1-x_4)(x_1-x_5)\\
&-(x_2-x_3)(x_2-x_4)(x_2-x_5)]\\
&+(x_3-x_1)(x_3-x_2)(x_3-x_4)(x_3-x_5)\\
&+(x_4-x_5)[-(x_1-x_4)(x_2-x_4)(x_3-x_4)\\
&+(x_1-x_5)(x_2-x_5)(x_3-x_5)].
\end{aligned}$$

由假设条件 $x_1 \geqslant x_2 \geqslant x_3 \geqslant x_4 \geqslant x_5$ 容易看出上式右边三项均不小于 0，于是 $A_5 \geqslant 0$，即 A_5 是正定的．这就证明了只有 A_3 和 A_5 是正定的．

我们已经看到 A_3 是实系数多项式的平方和．现在我们证明：A_5 不是实系数多项式的平方和．为此我们首先证明：

引理 4 设 $Q(x_1, \cdots, x_5) = \sum\limits_{1 \leq j \leq k \leq 5} c_{jk}x_jx_k$ 是实系数二次型，并且当变量 x_1, x_2, x_3, x_4, x_5 当中只要其中三个取相同值，而其余两个取相同值时，Q 均取值为零，则 Q 必恒为零．

证明 设 $x_1 = x_2 = y$, $x_3 = x_4 = x_5 = z$．由题设知

$$
\begin{aligned}
0 &= Q(y, y, z, z, z) \\
&= (c_{11}+c_{12}+c_{22})y^2 + (c_{13}+c_{14}+c_{15}+c_{23}+c_{24}+c_{25})yz \\
&\quad + (c_{33}+c_{44}+c_{55}+c_{34}+c_{35}+c_{45})z^2.
\end{aligned}
$$

由于上式对任意实数 y 和 z 均成立，从而上式右边关于 y^2, yz, z^2 的系数必恒为零．即

$$c_{11}+c_{12}+c_{22}=0, \qquad ⑧$$

$$c_{13}+c_{14}+c_{15}+c_{23}+c_{24}+c_{25}=0, \qquad ⑨$$

$$c_{33}+c_{44}+c_{55}+c_{34}+c_{35}+c_{45}=0. \qquad ⑩$$

如果我们取 $x_3 = x_4 = y$, $x_1 = x_2 = x_5 = z$，由题设知 Q 值仍为零．类似方法又得到系数之间一些关系，这些关系应当是⑧，⑨，⑩式中下标 1 和 3 互换，2 和 4 互换而得到的新公式．例如对应于⑧式我们现在得到

$$c_{33}+c_{34}+c_{44}=0, \qquad ⊛$$

从⑩式减去⊛式，得到 $c_{35}+c_{45}=-c_{55}$．由于题设条件关于 $x_1, x_2, \cdots, x_5$ 完全对称的．所以对于系数之间任意一个关系，将系数下标 1, 2, 3, 4, 5 作任意一个新的排列（或叫置换），得到新的关系也应当是对的．于是将已得到的 $c_{35}+c_{45}$

$=-c_{55}$ 中 4 和 5 不动, 3 和 2 互换, 1 也不动, 便得到新的关系 $c_{25}+c_{45}=-c_{55}$. 于是 $c_{25}=c_{35}$. 同样考虑便知:

$$c_{15}=c_{25}=c_{35}=c_{45}. \tag{11}$$

再作适当的下标置换又得到

$$\begin{aligned} c_{15}=c_{12}=c_{13}=c_{14}, \quad c_{12}=c_{23}=c_{24}=c_{25}, \\ c_{13}=c_{23}=c_{34}=c_{35}, \quad c_{14}=c_{24}=c_{34}=c_{45} \end{aligned} \tag{12}$$

由 ⑪ 和 ⑪ 式便知所有系数 $c_{ij}(1\leqslant i<j\leqslant 5)$ 均相同, 设这个公共值为 c, 由 ⑨ 式知 $6c=0$, 即 $c=0$. 于是 $c_{ij}(1\leqslant i<j\leqslant 5)$ 均为零. 而 $c_{55}=-(c_{35}+c_{45})=0$. 再由对称性即知 $c_{11}=c_{22}=c_{33}=c_{44}=c_{55}=0$. 从而 Q 的所有系数均为零, 即 Q 恒为零.

现在我们来证明 $A_5(x_1, x_2, \cdots, x_5)$ 不是实系数多项式平方和. 用反证法: 如果

$$A_5=Q_1(x_1, \cdots, x_5)^2+\cdots+Q_m(x_1, \cdots, x_5)^2,$$

其中 $Q_1, \cdots, Q_m$ 均是实系数多项式. 由于 A_5 的次数为 4, 仿照引理 3 的证明, 可知 $Q_1, \cdots, Q_m$ 次数均不超过 2. 设 $q_i(x_1, \cdots, x_n)$ 为 $Q_i(x_1, \cdots, x_n)$ 的二次项全体, 则由于 A_5 是四次齐次的, 从而必然 $A_5=q_1^2+\cdots+q_m^2$. 因此我们不妨一开始就可假设 $Q_1, \cdots, Q_m$ 均是二次齐次的, 即均是二次型. 由 A_5 的表达式易知当 $x_1, \cdots, x_5$ 中三个取值相同而另两个取值相同时, A_5 取值为零. 从而这时必然 $Q_1, \cdots, Q_m$ 均取值零. 即 $Q_1, \cdots, Q_m$ 均是满足引理 4 条件的二次型. 于是 $Q_1, \cdots, Q_m$ 均恒为零. 而 A_5 不恒为零, 这就导致矛盾. 从而证明了 A_5 不是实系数多项式的平方和.

注意 $A_5(x_1, \cdots, x_5)$ 虽然包含 5 个变量, 由于它只依赖变量的差 $x_i-x_j(i\neq j)$, 从而实际上 A_5 只依赖 4 个变量. 确切地说, 令

$$y_i=x_i-x_5 \quad (1\leqslant i\leqslant 4).$$

则当 $1\leqslant i\neq j\leqslant 4$ 时，$x_i-x_j=(x_i-x_5)-(x_j-x_5)=y_i-y_j$. 因此 A_5 可化成关于 y_1, y_2, y_3, y_5 的四次齐次多项式. 从而它给出 $P_{4,4}-\Sigma_{4,4}$ 中的一个具体例子.

【例 2】(林节玄，蔡文端，1977) $P_{4,4}-\Sigma_{4,4}$ 中更简单的例子为

$$Q(x, y, z, w)=w^4+x^2y^2+y^2z^2+z^2x^2-4xyzw.$$

这个多项式的正定性由算术平均值≥几何平均值立刻得出：$\frac{1}{4}(w^4+x^2y^2+y^2z^2+z^2x^2)\geqslant(w^4x^2y^2y^2z^2z^2x^2)^{\frac{1}{4}}=|wxyz|$. 从而 $Q\geqslant 0$. 现在设 Q 是多项式平方和，则

$$Q=Q_1(x, y, z, w)^2+\cdots+Q_m(x, y, z, w)^2. \qquad (*)$$

与上例一样，不妨设 $Q_i(x, y, z, w)$ $(1\leqslant i\leqslant m)$ 均是二次型. 由于 Q 中不包含 x^4, y^4, z^4 项，可知 Q_i 中均不包含 x^2, y^2, z^2 项. 因为若 $Q_i=a_ix^2+\cdots$, a_i 为实数，则 $0=x^4(a_1^2+\cdots+a_m^2)$，从而 $a_1=\cdots=a_m=0$. 然后我们又可推得 Q_i 均不包含 xw, yw, zw 诸项. 因为在 (*) 式中左边没有 x^2w^2 项，而当 $Q_i=b_ixw+\cdots$ 时，右边 x^2w^2 项系数为 $b_1^2+\cdots+b_m^2$(注意 Q_i 没有 x^2 项，从而右边 Q_i^2 中 x^2w^2 系数只能由 $(b_ixw)^2=b_i^2x^2w^2$ 得来). 于是 $b_1=\cdots=b_m=0$, 即 Q_i 不含 xw 项. 同样地 Q_i 不含 yw, zw 项. 于是 Q_i 中只有 xy, yz, zx 和 w^2 诸项. 但这样一来，Q_i^2 中便没有 $xyzw$ 项，即 (*) 式右边没有 $xyzw$ 项，而左边 Q 中有一项 $-4xyzw$，这便导致矛盾. 因此 Q 不为实系数多项式平方和. 这证明 $Q\in P_{4,4}-\Sigma_{4,4}$.

【例 3】(林节玄，蔡文端，1977) 现在给出 $P_{3,6}-\Sigma_{3,6}$ 中的例子：

$$S(x, y, z)=x^4y^2+y^4z^2+z^4x^2-3x^2y^2z^2,$$

$$S'(x, y, z)=z^6+x^4y^2+x^2y^4-3x^2y^2z^2.$$

由算术平均值≥几何平均值易知 S 和 S' 均是正定的. 设 $S=Q_1^2+\cdots+Q_m^2$. 与前一样, 不妨设 Q_i 均是关于 x, y, z 的三次齐次多项式. 由于 S 中无 x^6, y^6 和 z^6 诸项, 可知 Q_i 中无 x^3, y^3, z^3 诸项. 然后又可知道 Q_i 中无 xy^2, yz^2, zx^2 诸项, 其理由与例 2 相仿. 于是 $Q_i=a_ix^2y+b_iy^2z+c_iz^2x+d_ixyz(1\leqslant i\leqslant m)$. 但是这时 $Q_1^2+\cdots+Q_m^2$ 中 $x^2y^2z^2$ 的系数为 $d_1^2+\cdots+d_m^2\geqslant 0$, 而 S 中 $x^2y^2z^2$ 的系数为 -3, 这就导致矛盾. 从而 S 不是实系数多项式平方和. 即 $S\in P_{3,6}-\Sigma_{3,6}$.

练习 **1.** 用类似方法证明 $S'\in P_{3,6}-\Sigma_{3,6}$.

2. 设 $n\geqslant 3$,

$S_n(x_1, \cdots, x_n)=\sum_{i=1}^{n} x_i^{2n-2}x_{i+1}^2-nx_1^2\cdots x_n^2$（其中令 $x_{n+1}=x_1$）. 求证: $S_n\in P_{n,2n}-\Sigma_{n,2n}$.

3. 求证

$$x^4(x-y)(x-z)+y^4(y-x)(y-z)+z^4(z-x)(z-y)\in P_{3,6}-\Sigma_{3,6}.$$

【例 4】 (G. Stengle, 1979) 令

$$T(x, y, z)=x^3z^3+(y^2z-x^3-z^2x)^2,$$

求证: $T\in P_{3,6}-\Sigma_{3,6}$.

我们先证 T 是正定的. 若 $z=0$, 则 $T=x^6\geqslant 0$. 下设 $z\neq 0$. 由于 T 是齐次多项式, $T(\alpha x, \alpha y, \alpha z)=\alpha^6T(x, y, z)$. 所以我们不妨设 $z=1$. 这时当 $x\geqslant 0$ 时, $T(x, y, 1)=x^3+(y^2-x-x^3)^2\geqslant 0$. 而当 $x<0$ 时, $T(x, y, 1)\geqslant x^3+(x+x^3)^2\geqslant x^3+x^6+x^2\geqslant 0$（因为 x^6 和 x^2 必有一个 $\geqslant -x^3$）, 于是 T 正定. 再证 T 不是实系数多项式平方和. 假如

$$T(x, y, z)=Q_1(x, y, z)^2+\cdots+Q_m(x, y, z)^2,$$

其中 Q_i 可设均为三次齐次多项式. 由于这是关于 x, y, z 的恒等式, 我们可令 $z=1$, $y=\sqrt{x+x^3}$, 于是 $T(x, \sqrt{x+x^3}, 1)=x^3$. 而每个 Q_i 均可写成 $Q_i=A_i(x)+yB_i(x)$, 其中 $A_i(x)$

和 $B_i(x)$ 是 x 的实系数多项式(注意 $y^2=x+x^3$). 于是

$$x^3=\sum_{i=1}^{m}(A_i(x)+yB_i(x))=\sum_{i=1}^{m}(A_i^2(x)+(x+x^3)B_i^2(x))$$

$$+2y\sum_{i=1}^{m}A_i(x)B_i(x).$$

由于 $y=\sqrt{x^3+x}\notin\mathbf{R}(x)$, 可知

$$x^3=\sum_{i=1}^{m}A_i^2(x)+(x+x^3)\sum_{i=1}^{m}B_i^2(x).$$

代入 $x=0$, 可知 $0=\Sigma A_i^2(0)$. 但是 $A_i(0)$ 为实数, 从而必然 $A_i(0)=0(1\leqslant i\leqslant m)$, 即 $x|A_i(x)$ $(1\leqslant i\leqslant m)$. 令 $A_i(x)=x\alpha_i(x)$, 其中 $\alpha_i(x)$ 为实系数多项式, 则上式变成

$$x^2=x\Sigma\alpha_i^2(x)+(1+x^2)\Sigma B_i^2(x).$$

再代入 $x=0$, 则 $0=\Sigma B_i^2(0)$. 于是 $B_i(0)=0$, 即 $x|B_i(x)$. 令 $B_i(x)=x\beta_i(x)$, 其中 $\beta_i(x)$ 为实系数多项式$(1\leqslant i\leqslant m)$, 则

$$x=\Sigma\alpha_i^2(x)+x(1+x^2)\Sigma\beta_i^2(x).$$

同样又有 $x|\alpha_i(x)$. 令 $\alpha_i(x)=x\gamma_i(x)$ $(1\leqslant i\leqslant m)$, $\gamma_i(x)$ 为实系数多项式, 则 $1=x\Sigma\gamma_i^2(x)+(1+x^2)\Sigma\beta_i^2(x)$. 由于左边为 1, 从而 $\gamma_i(x)$, $\beta_i(x)$ $(1\leqslant i\leqslant m)$ 不能均为零. 但这时右边又是次数$\geqslant 1$ 的多项式, 从而导致矛盾. 这表明 $T\in P_{3,6}-\Sigma_{3,6}$.

练习 1. 对每个奇数 m, 求证: $T^m\in P_{3,6m}-\Sigma_{3,6m}$.

2. 对 $k\geqslant 1$, 令

$$T_k(x,y,z)=x^{2k+1}z^{2k+1}+(z^{2k-1}y^2-xz^{2k}-x^{2k+1})^2.$$

求证: $T_k\in P_{3,4k+2}-\Sigma_{3,4k+2}$.

【例 5】(蔡文端, 1975). 令

$$F(x_1,x_2,x_3,y_1,y_2,y_3)$$
$$=x_1^2y_1^2+x_2^2y_2^2+x_3^2y_3^2-2(x_1x_2y_1y_2+x_2x_3y_2y_3+x_3x_1y_3y_1)$$
$$+2(x_1^2y_2^2+x_2^2y_3^2+x_3^2y_1^2).$$

求证: $F\in P_{6,4}-\Sigma_{6,4}$.

先证 F 正定：由于将 $x_1, x_2, x_3, y_1, y_2, y_3$ 分别改成 $x_2, x_3, x_1, y_2, y_3, y_1$ 之后 F 式不变，并且 $|x_1|\leqslant|x_2|$，$|x_2|\leqslant|x_3|$ 和 $|x_3|\leqslant|x_1|$ 之中至少有一成立．我们可不妨假设 $|x_1|\leqslant|x_2|$．这时

$$F=(x_1y_1-x_2y_2+x_3y_3)^2+2x_1^2y_2^2+2(x_2^2y_3^2+x_3^2y_1^2-2x_1x_3y_1y_3)\geqslant 0.$$

如果 F 是实系数多项式平方和，则 $F=\Sigma f_i^2$，其中 f_i 是二次型．由于 F 中无 $x_1^2y_3^2$，$x_2^2y_1^2$，$x_3^2y_2^2$ 诸项，从而 f_i 中无 x_1y_3，x_2y_1，x_3y_2 诸项．于是 $f_i=g_i+h_i$，其中 $g_i=a_1x_1y_1+a_2x_2y_2+a_3x_3y_3$，$h_i=b_1x_1y_2+b_2x_2y_3+b_3x_3y_1$，$a_i, b_i$ 均为实数．代入 $F=\Sigma(g_i+h_i)^2$，可知

$$\Sigma g_ih_i=0,\quad \Sigma h_i^2=2(x_1^2y_2^2+x_2^2y_3^2+x_3^2y_1^2),$$

$$\Sigma g_i^2=x_1^2y_1^2+x_2^2y_2^2+x_3^2y_3^2-2(x_1x_2y_1y_2+x_2x_3y_2y_3+x_3x_1y_3y_1).$$

但最后一公式是不可能的，因为当 x_i，y_i 均取值为 1 时，右边为 -3，而左边 $\geqslant 0$．这一矛盾表明 $F\in P_{6,4}-\Sigma_{6,4}$．

3．构作 $s(F)=2^k$ 的域

设 F 是无序域，则 -1 为 F 中平方和．我们以 $s(F)$ 表示将 -1 表成 F 中元素平方和所需最少元素个数．我们在第三节曾经证明了费斯特定理的第(1)部分，即 $s(F)$ 只取值为 2 的方幂．本小节我们对每个 $k\geqslant 0$，均构作一个域 F，使得 $s(F)=2^k$．为此先作一些准备．

引理 5 设 F 为域，若不定方程 $x_1^2+\cdots+x_n^2=0$ 在域 F 中没有非零解，则该不定方程在多项式环 $F[x]$ 中也没有非零解（即不存在 n 个不全为零的多项式 $f_1(x), \cdots, f_n(x)\in F[x]$，使得 $f_1(x)^2+\cdots+f_n^2(x)=0$）．

证明 用反证法．假设有 $F[x]$ 中 n 个不全为零的多项式 $f_1(x)$, …, $f_n(x)$ 使得 $f_1(x)^2+\cdots+f_n^2(x)=0$. 如果 x 除尽所有的 $f_i(x)$ $(1\leqslant i\leqslant n)$，令 $f_i(x)=xg_i(x)$ $(1\leqslant i\leqslant n)$，则 $g_i(x)$ 是次数小于 $f_i(x)$ 的次数的多项式，并且 $g_1^2(x)+\cdots+g_n^2(x)=0$. 如果 x 又除尽所有的 $g_i(x)$ $(1\leqslant i\leqslant n)$．我们再令 $g_i(x)=xh_i(x)$ $(1\leqslant i\leqslant n)$．如此继续下去，由于多项式次数不能无限下降，从而我们总能得到多项式 $l_1(x)$, …, $l_n(x)\in F[x]$，使得 $l_1^2(x)+\cdots+l_n^2(x)=0$，并且 x 不能除尽所有 $l_i(x)$ $(1\leqslant i\leqslant n)$，即 $l_1(0)$, …, $l_n(0)$ 不全为零．但是 $l_1^2(0)+\cdots+l_n^2(0)=0$，而 $l_i(0)$ $(1\leqslant i\leqslant n)$ 是域 F 中 n 个不全为零的元素．这就与引理假设相矛盾．于是证明了引理．

引理 6 设 F 为域．我们以 $G_n(F[x])$ 表示 $F[x]$ 中可表成 $F[x]$ 中 n 个多项式平方和的多项式全体．设 α 为 F 中非零元素．如果 $\alpha\in G_n(F[x])$，则 $\alpha\in G_n(F)$．特别若 $-1\in G_n(F[x])$，则 $-1\in G_n(F)$．

证明 设 $\alpha\in G_n(F[x])$，即存在 $F[x]$ 中 n 个多项式 $f_1(x)$, …, $f_n(x)$，使得 $f_1^2(x)+\cdots+f_n^2(x)=\alpha$. 取 $x=0$，即得 $f_1^2(0)+\cdots+f_n^2(0)=\alpha$，而 $f_i(0)\in F$ $(1\leqslant i\leqslant n)$．这就证明了 $\alpha\in G_n(F)$．

我们在上小节曾经证明过(定理 1)：若实系数多项式 $f(x)$ 是正定的(即可表成有理函数的平方和)，则 f 也可表成关于 x 的实系数多项式的平方和．1963 年，英国数学家卡塞斯 (Cassels) 证明这对任何域 F 均对．即我们有

卡塞斯定理 设 F 为域，$p(x)$ 为 $F[x]$ 中非零多项式．若 $p(x)$ 可表成 $F(x)$ 中 n 个有理函数的平方和，则 $p(x)$ 也可表成 $F[x]$ 中 n 个多项式的平方和．(从而再加引理 6 便知，若 a 为 F 中元素并且 $p(a)\neq 0$，则 $p(a)$ 可表成 F 中元素的平方

和.)

证明 由假设知存在多项式 $f_0(x)$, $f_1(x)$, $\cdots$, $f_n(x)\in F[x]$, $f_0(x)\neq 0$, 使得

$$p(x)=\left(\frac{f_1(x)}{f_0(x)}\right)^2+\cdots+\left(\frac{f_n(x)}{f_0(x)}\right)^2. \qquad ㊟$$

我们设 $f_0(x)$ 是使上式成立的所有分母多项式中次数最小者,我们要证明 $f_0(x)$ 的次数为零, 即 $f_0(x)$ 为 F 中非零元素. 从而由 ㊟ 式即知 $p(x)$ 为 $F[x]$ 中 n 个多项式的平方和. 我们用反证法: 若 f_0 的次数$\geqslant 1$, 考虑域 $F(x)$ 上以 Y_0, Y_1, $\cdots$, Y_n 为变量的二次齐次方程:

$$\varphi(Y_0, Y_1, \cdots, Y_n)=-p(x)Y_0^2+Y_1^2+\cdots+Y_n^2=0.$$

由 ㊟ 式知 $(Y_0, Y_1, \cdots, Y_n)=(f_0, f_1, \cdots, f_n)$ 为此方程的解, 即 $\varphi(f_0, \cdots, f_n)=0$. 令 $a_0=-p(x)$, $a_1=\cdots=a_n=1$, 则 $\varphi(Y_0, \cdots, Y_n)$ 可写成 $a_0Y_0^2+\cdots+a_nY_n^2$. 现在用 $f_0(\neq 0)$ 去除每个 $f_i(1\leqslant i\leqslant n)$, 则有除法算式

$$f_i(x)=g_i(x)f_0(x)+r_i(x) \quad (1\leqslant i\leqslant n).$$

其中多项式 $r_i(x)$ 或者为零, 或者 $r_i(x)$ 次数小于 $f_0(x)$ 的次数. 由 $f_0(x)$ 的次数最小性可知 $f_0(x)$ 不能除尽所有 $f_i(x)$, 即 $r_i(x)$ $(1\leqslant i\leqslant n)$ 不全为零. 再规定 $g_0(x)=1$, $r_0(x)=0$, 则也有 $f_0(x)=g_0(x)f_0(x)+r_0(x)$. 现在令

$$h_i(x)=f_i(x)\sum_{j=0}^{n}a_jg_j^2(x)-2g_i(x)\sum_{j=0}^{n}a_jf_j(x)g_j(x)$$
$$(0\leqslant i\leqslant n),$$

则

$$\varphi(h_0, h_1, \cdots, h_n)=\sum_{i=0}^{n}a_ih_i^2$$
$$=\sum_{i=0}^{n}a_i\left[f_i\sum_{j=0}^{n}a_jg_j^2-2g_i\sum_{j=0}^{n}a_jf_jg_j\right]^2$$

$$=\sum_{i=0}^{n}a_i\Big[f_i^2\Big(\sum_{j=0}^{n}a_jg_j^2\Big)^2-4f_ig_i\Big(\sum_{j=0}^{n}a_jg_j^2\Big)\Big(\sum_{j=0}^{n}a_jf_jg_j\Big)$$

$$+4g_i^2\Big(\sum_{j=0}^{n}a_jf_jg_j\Big)^2\Big]$$

$$=\Big(\sum_{i=0}^{n}a_if_i^2\Big)\Big(\sum_{j=0}^{n}a_jg_j^2\Big)^2-4\Big(\sum_{j=0}^{n}a_jg_j^2\Big)\Big(\sum_{j=0}^{n}a_jf_jg_j\Big)^2$$

$$+4\Big(\sum_{i=0}^{n}a_ig_i^2\Big)\Big(\sum_{j=0}^{n}a_jf_jg_j\Big)^2$$

$$=\Big(\sum_{i=0}^{n}a_if_i^2\Big)\Big(\sum_{j=0}^{n}a_jg_j^2\Big)^2=0.$$

这是由于 $\sum_{i=0}^{n}a_if_i^2=\varphi(f_0,\cdots,f_n)=0$. 于是 $-p(x)h_0^2+h_1^2+\cdots+h_n^2=0$. 但是

$$h_0(x)=f_0\sum_{i=0}^{n}a_ig_i^2-2g_0\sum_{i=0}^{n}a_if_ig_i$$

$$=f_0\Big(-pg_0^2+\sum_{i=1}^{n}g_i^2\Big)-2g_0\Big(-pf_0g_0+\sum_{i=1}^{n}a_if_ig_i\Big)$$

$$=pf_0+\sum_{i=1}^{n}(f_0g_i^2-2f_ig_i)$$

$$=\frac{1}{f_0}\Big[pf_0^2+\sum_{i=1}^{n}(f_0^2g_i^2-2f_0g_if_i)\Big]$$

$$=\frac{1}{f_0}\Big[pf_0^2+\sum_{i=1}^{n}(f_0g_i-f_i)^2-\sum_{i=1}^{n}f_i^2\Big]$$

$$=\frac{1}{f_0}\sum_{i=1}^{n}(f_0g_i-f_i)^2=\frac{1}{f_0}\sum_{i=1}^{n}r_i^2.$$

我们以 $\deg f(x)$ 表示多项式 $f(x)$ 的次数，则由上式知

$$\deg h_0\leqslant 2\cdot\max_{1\leqslant i\leqslant n}\deg r_i-\deg f_0$$

$$<2\deg f_0-\deg f_0=\deg f_0,$$

即 h_0 的次数小于 f_0 的次数. 由于 $r_i(1\leqslant i\leqslant n)$ 不全为零，从而 $h_0(x)=\frac{1}{f_0}\sum_{i=1}^{n}r_i^2\neq0$，即 $h_0(x)$ 是非零多项式，并且有

$p(x)=\left(\frac{h_1}{h_0}\right)^2+\cdots+\left(\frac{h_n}{h_0}\right)^2$，这就与 f_0 的次数最小性相矛盾．由此证明了卡塞斯定理．

注记：这个定理的证明关键是利用了多项式环 $F[x]$ 有除法算式．作为一个练习，请大家采用整数环 $\mathbf{Z}$ 中的除法算式并仿照上面定理的证法来直接证明：若正整数 n 是三个有理数的平方和，则必是三个整数的平方和．我们过去曾用关于三整数平方和可表性的高斯定理证明过这个结果．

上述定理的一个直接推论是：

引理7 设 F 为域，$p(x_1, \cdots, x_n)=\frac{f(x_1, \cdots, x_n)}{g(x_1, \cdots, x_n)}$，其中 $f(x_1, \cdots, x_n)$，$g(x_1, \cdots, x_n)\in F[x_1, \cdots, x_n]$．令 $e_1, \cdots, e_n\in F$，使得 $g(e_1, \cdots, e_n)\neq 0$，$f(e_1, \cdots, e_n)\neq 0$．如果 $p(x_1, \cdots, x_n)$ 是 $F(x_1, \cdots, x_n)$ 中 n 个有理函数的平方和，则 $p(e_1, \cdots, e_n)$ 为 F 中 n 个元素的平方和．

证明 由假设知多项式 $f(x_1, \cdots, x_n)g(x_1, \cdots, x_n)$ 为 $F(x_1, \cdots, x_n)$ 中 n 个有理函数的平方和．我们现在对此引理作归纳法证明．当 $n=1$ 时，由于 $f(x_1)g(x_1)$ 为 n 个有理函数平方和，采用上面定理即知多项式 $f(x_1)g(x_1)$ 也是 $F[x_1]$ 中 n 个多项式的平方和．于是代入 $x_1=e_1$，即知 $f(e_1)g(e_1)$ 是 F 中 n 个元素的平方和，从而 $p(e_1)=\frac{f(e_1)g(e_1)}{g(e_1)^2}$ 也是如此，即 $n=1$ 时引理正确．现在设 $n\geqslant 2$，并且假设引理对 $n-1$ 时成立．令 $F'=F(x_1, \cdots, x_{n-1})$，则 $F(x_1, \cdots, x_n)=F'(x_n)$．由刚证明的 $n=1$ 的情形（但是用域 F' 作为前面的 F，即 f 和 g 均看成系数属于 F' 的关于 x_n 的多项式），便知 $f(x_1, \cdots, x_{n-1}, e_n)g(x_1, \cdots, x_{n-1}, e_n)$ 是域 F' 中 n 个元素的平方和．现在 $f(x_1, \cdots, x_{n-1}, e_n)g(x_1, \cdots, x_{n-1}, e_n)$ 为 $F[x_1, \cdots, x_{n-1}]$

中 $n-1$ 个变量的多项式. 再用归纳假设即知 $f(\theta_1, \cdots, \theta_n)$ $g(\theta_1, \cdots, \theta_n)$ 为域 F 上 n 个元素的平方和，从而 $p(\theta_1, \cdots, \theta_n) = \frac{f(\theta_1, \cdots, \theta_n)}{g(\theta_1, \cdots, \theta_n)}$ 也是如此. 证毕.

引理 8 设 $n\geqslant 2$, F 为域, $-1\notin G_{n-1}(F)$, d 为 F 中非零元素. 则 d 为 F 中 $n-1$ 个元素的平方和 $\Leftrightarrow d+x^2$ 为 $F(x)$ 中 n 个元素的平方和.

证明 若左边成立，则右边显然成立. 现在设 $d+x^2$ 为 $F(x)$ 中 n 平方和. 由 Cassels 定理, $d+x^2$ 也为 $F[x]$ 中 n 个多项式的平方和. 于是

$$d+x^2=f_1(x)^2+\cdots+f_n(x)^2, \qquad ⊛$$

其中 $f_i(x)\in F[x]\,(1\leqslant i\leqslant n)$. 设 $f_i(x)\,(1\leqslant i\leqslant n)$ 的次数的最大值为 d，则 $f_i(x)=a_ix^d+\cdots$, 其中 $a_i\in F$, 并且 $a_i(1\leqslant i\leqslant n)$ 不全为零. 如果 $d\geqslant 2$, 则将 ⊛ 式右边展开并比较等式两边 x^{2d} 的系数(注意 $d\geqslant 2$ 时, $2d\geqslant 4$), 即得

$$0=a_1^2+\cdots+a_n^2.$$

由于 $a_i(1\leqslant i\leqslant n)$ 不全为零，由此推出 $-1\in G_{n-1}(F)$，而这与假设矛盾. 由此可知 $d\leqslant 1$, 即 $f_i(x)=a_i+b_ix$, 其中 a_i, $b_i\in F(1\leqslant i\leqslant n)$. 方程 $a_1+b_1x=x$ 和 $a_1+b_1x=-x$ 必至少有一个在 F 中可解，因为 b_1+1 和 b_1-1 不能均为零. 因此存在 $c\in F$，使得 $a_1+b_1c=c$ 或 $-c$. 将 $x=c$ 代入 ⊛ 式，则得到

$$d+c^2=(\pm c)^2+f_2(c)^2+\cdots+f_n(c)^2,$$

即 $d=f_2(c)^2+\cdots+f_n(c)^2$. 于是 d 为 F 中 $n-1$ 个元素的平方和. 证毕.

引理 9 设 F 为域, $-1\notin G_{n-1}(F)$. 则 $1+x_1^2+\cdots+x_n^2$ 不为 $F(x_1, \cdots, x_n)$ 中的 n 平方和, $x_1^2+x_2^2+\cdots+x_{n+1}^2$ 不为 $F(x_1, \cdots, x_{n+1})$ 中的 n 平方和.

证明 易知 $1+x_1^2$ 不为 $F(x_1)$ 中元素的平方. 现在对 n 归纳证明 $1+x_1^2+\cdots+x_n^2\notin G_n(F(x_1, \cdots, x_n))$. 设 $n\geqslant 2$, 并且命题对 $n-1$ 成立. 由于 $-1\notin G_{n-1}(F)$, 从而 $-1\notin G_{(n-1)-1}(F)$. 由归纳假设知 $1+x_1^2+\cdots+x_{n-1}^2=d$ 不是域 $F'=F(x_1, \cdots, x_{n-1})$ 中 $(n-1)$ 个元素的平方和. 如果再能证明 $-1\notin G_{n-1}(F')$, 由引理 8 即知 $1+x_1^2+\cdots+x_n^2=d+x_n^2$ 不是域 $F(x_1, \cdots, x_n)=F'(x_n)$ 中 n 平方和. 但是若 $-1\in G_{n-1}(F')=G_{n-1}(F(x_1, \cdots, x_{n-1}))$, 由引理 7 推出 $-1\in G_{n-1}(F)$, 这与假设矛盾. 于是就证明了当 $-1\notin G_{n-1}(F)$ 时 $1+x_1^2+\cdots+x_n^2$ 不是 $F(x_1, \cdots, x_n)$ 中 n 平方和.

同样地, 易知 $x_1^2+x_2^2$ 不是 $F(x_1, x_2)$ 中元素的平方. 然后对 n 归纳即知 $x_1^2+x_2^2+\cdots+x_{n+1}^2$ 不是 $F(x_1, \cdots, x_{n+1})$ 中的 n 个元素的平方和.

注记: 特别对于任意有序域 F, -1 不是 F 中平方和. 从而上面引理中的结论对于任意有序域 F 都是对的.

引理 10 设 F 是有序域, d 为 F 中非零元素, $K=F(\sqrt{-d})$ 为无序域. 若 $s(K)=s$(由于 K 无序知 s 是有限的, 即 s 为正整数), 则 $d\in G_{2s-1}(F)$.

证明 由 $s(K)=s$, 可知存在 b_i, $c_i\in F\ (1\leqslant i\leqslant s)$, 使得

$$-1=\sum_{i=1}^{s}(b_i+c_i\sqrt{-d})^2$$

$$=\sum_{i=1}^{s}(b_i^2-dc_i^2)+\left(2\sum_{i=1}^{s}b_ic_i\right)\sqrt{-d}.$$

由于 F 是有序域而 K 是无序域, 从而 $K\neq F$, 即 $\sqrt{-d}\notin F$. 于是必然 $\sum_{i=1}^{s}b_ic_i=0$, $-1=\sum_{i=1}^{s}b_i^2-dt$, 其中 $t=\sum_{i=1}^{s}c_i^2\in F$. 如果 $t=0$, 则 $\sum_{i=1}^{s}c_i^2=0$. 但是 F 为有序域, 从而 $c_i\ (1\leqslant i\leqslant n)$ 均

为零. 于是 $-1=\sum_{i=1}^{s} b_i^2$, 而这又与 F 是有序域相矛盾. 因此 $t\neq 0$, 于是 $dt^2=t+t\left(\sum_{i=1}^{s} b_i^2\right)$. 但是由费斯特定理的第 (1) 部分, s 为 2 的方幂, 并且这时我们已经证明了

$$t\left(\sum_{i=1}^{s} b_i^2\right)=\left(\sum_{i=1}^{s} c_i^2\right)\left(\sum_{i=1}^{s} b_i^2\right)=A_1^2+\cdots+A_s^2,$$

其中 $A_i(1\leqslant i\leqslant s)\in F$, 并且 $A_1=\sum_{i=1}^{s} b_ic_i=0$, 于是 $t\left(\sum_{i=1}^{s} b_i^2\right)\in G_{s-1}(F)$. 而 $t=\left(\sum_{i=1}^{s} c_i^2\right)\in G_s(F)$, 从而 $dt^2=t+t\left(\sum_{i=1}^{s} b_i^2\right)\in G_{2s-1}(F)$, 从而 $d\in G_{2s-1}(F)$. 证毕.

现在我们可以证明费斯特定理的第(2)部分. 即对每个 $k\geqslant 0$, 构作域 F, 使得 $s(F)=2^k$. 显然对于复数域 $\mathbf{C}$, $s(\mathbf{C})=1$, 以下设 $k\geqslant 1$.

定理 3 设 F 为有序域, d 为 F 中非零元素, $k\geqslant 1$, $2^k\leqslant n<2^{k+1}$, $d\in G_n(F)$, $d\notin G_{n-1}(F)$. $K=F(\sqrt{-d})$. 则 $s(K)=2^k$.

证明 由于 $-(\sqrt{-d})^2=d\in G_n(F)\subseteq G_n(K)$, 从而 $-1\in G_n(K)$, 于是 $s(K)\leqslant n<2^{k+1}$. 由于 $s(K)$ 为 2 的方幂, 因此 $s(K)\leqslant 2^k$. 另一方面, 若 $s(K)<2^k$, 则 $s(K)\leqslant 2^{k-1}$. 由上面引理 10 可知 $d\in G_{2(2^{k-1})-1}(F)=G_{2^k-1}(F)\subseteq G_{n-1}(F)$, 而这与假设 $d\notin G_{n-1}(F)$ 矛盾. 证毕.

特别地:

定理 4 设 F_0 为任意有序域 (例如取 $F_0=\mathbf{R}$), $F=F_0(x_1,\cdots,x_n)$, 其中

$$2^k\leqslant n<2^{k+1},\quad k\geqslant 1.$$

$$d=x_1^2+\cdots+x_n^2,\quad K=F(\sqrt{-d}),$$

则 $s(K)=2^k$.

证明 由引理 9 知 $d\in G_n(F)$, $d\notin G_{n-1}(F)$. 再由上面定理即得结果.

于是我们对任何正整数 k, 给出了使 $s(K)=2^k$ 的具体域 K 的例子.

4. 进一步的结果和未解决的问题

我们已经向大家介绍了关于平方和的许多有趣结果，其中很多结果的证明相当初等，我们向大家讲述了这些证明. 还有许多结果的证明超出了本书的允许范围. 另一方面，仍有不少关于平方和的问题至今没有解决. 作为本书的结尾，我们挑选其中容易叙述(不等于容易解决)的几个问题作一个简单的介绍.

I 我们从希尔伯特第 17 问题谈起. 这个问题由阿廷解决，即阿廷证明了：每个正定实系数多项式 $f(x_1, \cdots, x_n)$ 均是实系数有理函数的平方和. 现在我们试图把实系数域 $\mathbf{R}$ 改成任意有序域 K. 由于有序域 K 中可能有许多序，所以正定概念自然要作如下推广.

定义 设 K 是有序域. 系数属于 K 的多项式 $f(x_1, \cdots, x_n)$ 叫作是全正的，是指对 K 中任意元素 $a_1, \cdots, a_n$，如果 $f(a_1, \cdots, a_n)\neq 0$，则 $f(a_1, \cdots, a_n)$ 必是 K 中全正元素(即对于 K 的每个序 $f(a_1, \cdots, a_n)$ 均是正元素).

当 $K=\mathbf{R}$ 时，由于实数域 $\mathbf{R}$ 只有一个序，从而 $\mathbf{R}$ 上的全正多项式就是通常所说的正定多项式.

如果 $f(x_1, \cdots, x_n)$ 是 $K(x_1, \cdots, x_n)$ 中有理函数平方和，易知 $f(x_1, \cdots, x_n)$ 必是全正的. 反过来要问：

设 K 是有序域，$K[x_1, \cdots, x_n]$ 中每个全正多项式是否

一定为 $K(x_1, \cdots, x_n)$ 中有理函数的平方和?

阿廷的结果表明当 $K=\mathbf{R}$ 时这是对的. 可以证明当 K 是任意代数数域(特别当 K 是有理数域 $\mathbf{Q}$ 时)这也是对的. 但是 D. W. Dubois 于 1967 年构作了一个域 F, 它只有一个序, 但是存在系数属于 F 的二变量多项式 $f(x, y)$, 它对于 F 中唯一的序是正定的, 但不能表成 $F(x, y)$ 中有理函数的平方和. 从而提供了一个反例. 对于哪些有序域上述问题具有肯定答案, 人们还不完全清楚.

注意若 K 是无序域, 则 $K(x_1, \cdots, x_n)$ 也是无序域, 从而 $K(x_1, \cdots, x_n)$ 中每个有理函数均是平方和.

下面所述问题均于域的另一个重要数值有关, 叫作域的高度.

定义 设 K 为域. 如果存在正整数 n, 使得 K 中每个可表成平方和的元素均能表成 n 平方和, 那么满足此条件的最小 n 值叫作域 K 的高度, 表示成 $h(K)$. 如果不存在上述 n, 则记成 $h(K)=\infty$.

我们先举几个简单的例子:

【例 1】 $h(\mathbf{C})=1$. 因为每个复数 α 在 $\mathbf{C}$ 中均可开平方, 即存在复数 β, 使得 $\alpha=\beta^2$.

【例 2】 $h(\mathbf{R})=1$. 因为只有 0 和正实数才能表成实数的平方和, 而对每个正实数 α, $\sqrt{\alpha}$ 仍是实数, 而 $\alpha=(\sqrt{\alpha})^2$.

【例 3】 $h(\mathbf{Q})=4$. 只有 0 和正有理数才能表成有理数的平方和. 由于每个正整数均可表成四个整数平方和(拉格朗日定理), 由此易知每个正有理数均可表成四个有理数的平方和, 即 $h(\mathbf{Q})\leqslant 4$. 另一方面, 我们已经证明过, 若正整数 n 可表成三个有理数的平方和, 则 n 也必能表成三个整数的平方和. 但是我们知道 7 不是三整数平方和, 从而 $h(\mathbf{Q})>3$. 于

是 $h(\mathbf{Q})=4$.

可以证明，对每个代数数域 K，均有 $h(K)\leqslant 4$.

【例 4】 若 F 是无序域，$s(F)=s$（即 -1 为 F 中 s 平方和但不是 $(s-1)$ 平方和．由费斯特定理知 s 为 2 的方幂）．则 $h(F)=s$ 或者 $s+1$.

证明：若 $-1=a_1^2+\cdots+a_s^2$, $a_i\in F$，则对 F 中每个元素 α，

$$\alpha=\left(\frac{\alpha+1}{2}\right)^2-\left(\frac{\alpha-1}{2}\right)^2$$
$$=\left(\frac{\alpha+1}{2}\right)^2+\left(\frac{\alpha-1}{2}a_1\right)^2+\cdots+\left(\frac{\alpha-1}{2}a_s\right)^2,$$

即 α 为 $(s+1)$ 平方和．于是 $h(F)\leqslant s+1$．另一方面，-1 不是 $(s-1)$ 平方和，从而 $h(F)\geqslant s$．从而 $h(F)=s$ 或 $s+1$.

事实上，$h(F)=s(F)$ 和 $h(F)=s(F)+1$ 均可能发生．例如对 $F=\mathbf{C}$，则 $s(F)=h(F)=1$．而对 $F=\mathbf{C}[i]$，则 $s(F)=1$，但是 $i=\sqrt{-1}$ 不为 $\mathbf{Q}[i]$ 中完全平方，因为

$$\sqrt{i}=\pm\frac{1}{\sqrt{2}}(1+i)\notin\mathbf{Q}[i],$$

从而 $h(F)>1$，于是 $h(F)=2=s(F)+1$.

【例 5】 设 $F=\mathbf{R}(x_1, x_2, \cdots, x_n, \cdots)$，即包含无限个变量 $x_1, x_2,\cdots, x_n,\cdots$ 的实系数有理函数域．由上小节引理 9 知道 $1+x_1^2+\cdots+x_n^2$ 不是 $\mathbf{R}(x_1, \cdots, x_n)$ 中 n 平方和，易知它也不是域 F 中 n 平方和．由于 n 可任意大，这就表明 $h(F)=\infty$.

以上我们对一些域决定出其高度值．但是对于多数域，其高度的确切值至今不知．特别吸引人的是下述问题：

给了域 F 和正整数 n，试决定有理函数域 $F(x_1, \cdots, x_n)$ 的高度．特别地，$h(F(x_1, \cdots, x_n))$ 是如何依赖于 n 和域 F

的?这问题甚至对于两个简单的域 $F=\mathbf{R}$ 和 $\mathbf{Q}$ 均未解决.

II ($F=\mathbf{R}$ 的情形) 我们在上小节证明了 $1+x_1^2+\cdots+x_n^2$ 不是 $\mathbf{R}(x_1, \cdots, x_n)$ 中的 n 平方和, 因此 $h(\mathbf{R}(x_1, \cdots, x_n))\geqslant n+1$. 另一方面, 费斯特于 60 年代发展了一套关于二次型的代数理论. 利用这个理论他巧妙地证明了 $\mathbf{R}(x_1, \cdots, x_n)$ 中每个正定有理函数 $f(x_1, \cdots, x_n)$ 均是 $\mathbf{R}(x_1, \cdots, x_n)$ 中的 2^n 平方和, 即证明了 $h(\mathbf{R}(x_1, \cdots, x_n))\leqslant 2^n$.

当 $n=1$ 时, 由上述两个结果即知 $h(\mathbf{R}(x))=2$. 事实上, 这就是我们第 2 小节中的定理 1. 当 $n=2$ 时, 上述二结果表明 $3\leqslant h(\mathbf{R}(x, y))\leqslant 4$. 1976 年, 卡塞斯、费斯特等三人利用椭圆曲线理论证明了正定多项式

$$f(x, y)=1+x^2y^4+x^4y^2-3x^2y^2$$

不是 $\mathbf{R}(x, y)$ 中三平方和, 于是 $h(\mathbf{R}(x, y))=4$.

当 $n\geqslant 3$ 时, 目前只知 $1+n\leqslant h(\mathbf{R}(x_1, \cdots, x_n))\leqslant 2^n$, 没有决定出 $h(\mathbf{R}(x_1, \cdots, x_n))$ 的确切值来.

III ($F=\mathbf{Q}$ 的情形). 1906 年, 朗道(Landau)证了 $\mathbf{Q}(x)$ 中每个正定多项式均为 $\mathbf{Q}(x)$ 中 8 平方和. 1971 年, Pourchet 证明了 $\mathbf{Q}(x)$ 中正定多项式均为 $\mathbf{Q}(x)$ 中 5 平方和, 并且 5 是最好可能. 换句话说, 他证明了 $h(\mathbf{Q}(x))=5$. 事实上, 他在文章中证明了对任意代数数域 K, $h(K(x))\leqslant 5$. 人们猜想 $h(\mathbf{Q}(x_1, \cdots, x_n))\leqslant 2^n+3$. 当 $n=0$ 和 1 时我们知道等式成立, 但是对 $n\geqslant 2$ 情形不知这猜想是否正确, 更不知 $h(\mathbf{Q}(x_1, \cdots, x_n))$ 的确切值是多少.

练习 设 F 是无序域, $s(F)=s$, 求证 $h(F(x))=s+1$. 特别地, $h(\mathbf{C}(x_1, \cdots, x_n))=2$, $h(\mathbf{Q}[i](x_1, \cdots, x_n))=3$.

附录：一点初等数论

在这个附录里，我们讲一点本书所需要的初等数论符号、基本概念和结果，关于结果的证明可见任何一本初等数论参考书. 初等数论的出发点是：

算术基本定理 每个大于 1 的正整数 n 均可唯一(不计因子次序)地写成有限个素数乘积：

$$n=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}. \quad ①$$

其中 $p_1, p_2, \cdots, p_s$ 为不同的素数，$r_1, r_2, \cdots, r_s$ 为正整数. ①式叫作 n 的*标准分解式*.

整除 设 a 和 b 是整数，$a\neq 0$. 如果 $\frac{b}{a}$ 为整数，则称 a *整除* b，表示成 $a|b$. 否则，即 a 不能整除 b，表示成 $a\nmid b$. 当 $a|b$ 时，a 叫 b 的因子，b 叫 a 的倍数. 非零整数 $a_1, a_2, \cdots, a_n$ 的最大公因子和最小公倍数分别记作 $(a_1, a_2, \cdots, a_n)$ 和 $[a_1, a_2, \cdots, a_n]$. 如果 $(a, b)=1$，则称 a 和 b *互素*.

同余性质 设 m 为正整数. 整数 a 和 b 称作模 m 同余，是指 $m|a-b$，表示成 $a\equiv b \pmod m$. 同余式有如下运算性质：

(1) 若 $a\equiv b \pmod m$，$c\equiv d \pmod m$，则

$$a\pm c\equiv b\pm d \pmod m, \quad ac\equiv bd \pmod m.$$

(2) 若 $ac\equiv bc \pmod m$，并且 $(c, m)=1$，则

$$a\equiv b \pmod m.$$

(3) 若 $(a, m)=1$，则存在整数 a'，使得 $aa'\equiv 1 \pmod{m}$，并且 a' 在模 m 的意义下是唯一的。

所有整数按模 m 分成 m 个同余类。同一类中任意二数彼此模 m 同余，不同类中的数彼此模 m 不同余。每个同余类中取出一个数作为代表，m 个代表组成一个模 m 的完全剩余系。例如 $\{0, 1, 2, \cdots, m-1\}$ 便是模 m 的一个完全剩余系。当 m 为奇数时，$\left\{-\frac{m-1}{2}, -\frac{m-3}{2}, \cdots, -1, 0, 1, \cdots, \frac{m-3}{2}, \frac{m-1}{2}\right\}$ 也是模 m 的完全剩余系，因此当 m 为奇数时，对每个整数 a，均存在 b，使得 $a\equiv b \pmod{m}$，并且 $|b|<\frac{m}{2}$。

设 p 为奇素数，$p\nmid a$。如果同余方程 $x^2\equiv a \pmod{p}$ 可解，则称 a 是模 p 的二次剩余。否则便称为二次非剩余。模 p 的二次剩余(类)有 $\frac{p-1}{2}$ 个，它们是 $1^2, 2^2, 3^2, \cdots, \left(\frac{p-1}{2}\right)^2$ (所在的同余类)，从而模 p 的二次非剩余也有 $\frac{p-1}{2}$ 个。两个模 p 二次剩余之积及两个模 p 二次非剩余之积均是二次剩余；而一个模 p 二次剩余和一个二次非剩余之积是二次非剩余。如果我们引入记号

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{若 } a \text{ 为模 } p \text{ 二次剩余,}\\ -1, & \text{若 } a \text{ 为模 } p \text{ 二次非剩余.}\end{cases}$$

则上面结论可简写成

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right) \quad (\text{当 } p\nmid ab \text{ 时}).$$

$\left(\frac{a}{p}\right)$ 叫作勒让得(Legendre)符号。下面是初等数论又一个重要结果，它可用来有效地计算勒让得符号值，虽然它在数论中的地位和作用远远不仅如此。

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1, & 若\ p\equiv1(\bmod 4),\\ -1, & 若\ p\equiv3(\bmod 4).\end{cases}$$

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & 若\ p\equiv\pm1(\bmod 8),\\ -1, & 若\ p\equiv\pm3(\bmod 8).\end{cases}$$

（二次互反律） 设 p 和 q 是不同的奇素数，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=\begin{cases}-1, & 若\ p\equiv q\equiv3(\bmod 4),\\ 1, & 否则.\end{cases}$$

一次不定方程 设 $a_1, a_2, \cdots, a_m$ 是 m 个非零整数，并且 $(a_1, a_2, \cdots, a_m)=1$. 则对每个整数 n，不定方程

$$a_1x_1+a_2x_2+\cdots+a_mx_m=n$$

必有整数解 $(x_1, x_2, \cdots, x_m)$.

素数 素数在正整数集合中的分布特性是解析数论的一个中心议题. 早在公元前三世纪，欧几里得便证明了存在无穷多个素数（反证法：如果只有有限多个素数 $p_1, p_2, \cdots, p_s$，如何把 $p_1\cdots p_s+1$ 分解成素数乘积？）我们在本书中还需要比它再精细一点的事实，但是证明却很不简单.

狄里赫利(Dirichlet)算术级数中的素数定理 设 k 和 l 是两个互素的正整数，$1\leqslant l\leqslant k-1$. 则在算术级数（或叫等差数列）

$$\{l, l+k, l+2k, l+3k, \cdots\}=\{l+nk \mid n\geqslant0\}$$
$$=\{n\ 为正整数 \mid n\equiv l(\bmod k)\}$$

中存在无穷多个素数.